DOCUMENT RESUME

ED 372 748 IR 016 706

TITLE	Standards for Data Exchange and Case Management Information Systems in Support of Comprehensive Integrated School-Linked Services. Version 2.0.
INSTITUTION	Far West Lab. for Educational Research and Development, San Francisco, Calif.; Youth Law Center, San Francisco, CA.
SPONS AGENCY	California State Dept. of Education, Sacramento.; California State Dept. of Health, Sacramento.
PUB DATE	28 Mar 94
NOTE	209p.; The California Interagency Data Collaboration participated in the preparation of this report. Funding also provided by the Foundation Consortium for School-Linked Services.
PUB TYPE	Guides - Non-Classroom Use (055) -- Reports - Evaluative/Feasibility (142)
EDRS PRICE	MF01/PC09 Plus Postage.
DESCRIPTORS	*Case Records; Computer Software; *Confidentiality; Databases; Data Collection; Delivery Systems; Elementary Secondary Education; Federal Legislation; Guides; *Information Systems; *Information Utilization; *Standards; State Programs; Vendors
IDENTIFIERS	California; *Case Management; Data Management; Integrated Services; *School Linked Services

ABSTRACT

This report is intended as a guide for local comprehensive integrated school-linked services sites and software vendors in developing and implementing case management information systems for the exchange and management of client data. The report is also intended to influence new development and future revisions of data systems, databases, and reporting requirements of related state agencies and programs. As a first report of the California Interagency Data Collaboration, it addresses the objectives of reducing the data collection burden for case managers and facilitating the local use of data by developing standards for data translation in sharing, functional specifications, and confidentiality and the protection of privacy. These standards are itemized. One table and one figure illustrate the discussion. Appendixes list the race and ethnicity codes and federal and state statutes and regulations about confidentiality. (SLD)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

IR

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☐ This document has been reproduced as received from the person or organization originating it
☐ Minor changes have been made to improve reproduction quality
- Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

ED 372 748

CALIFORNIA INTERAGENCY DATA COLLABORATION

STANDARDS FOR DATA EXCHANGE AND CASE MANAGEMENT INFORMATION SYSTEMS

IN SUPPORT OF

COMPREHENSIVE INTEGRATED SCHOOL-LINKED SERVICES

VERSION 2.0

March 28, 1994

IR016706

BEST COPY AVAILABLE

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
T. Ross
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

Far West Laboratory for Educational Research and Development
730 Harrison Street, San Francisco, CA 94107-1242 (415) 565-3000

CALIFORNIA INTERAGENCY DATA COLLABORATION

STANDARDS FOR DATA EXCHANGE AND CASE MANAGEMENT INFORMATION SYSTEMS

IN SUPPORT OF

COMPREHENSIVE INTEGRATED SCHOOL-LINKED SERVICES

VERSION 2.0

March 28, 1994

This report was prepared by Far West Laboratory for Educational Research and Development, the Youth Law Center, and the California Interagency Data Collaboration. Funding was provided by the Foundation Consortium for School-linked Services in partnership with the California Departments of Education and Health Services. Member foundations of the consortium include the Arco Foundation, California Wellness Foundation, East Bay Community Foundation, Fleischhacker Foundation, Walter & Elise Haas Fund, William Randolph Hearst Foundation, Hewlett Foundation, Walter S. Johnson Foundation, Kaiser Family Foundation, Marin Community Foundation, San Diego Community Foundation, Sierra Health Foundation, Stuart Foundations, The San Francisco Foundation, and the Zellerbach Family Fund.

EXECUTIVE SUMMARY

This report is intended as a guide for local comprehensive integrated school-linked services (CISLS) sites and software vendors in developing and implementing case management information systems for the exchange and management of client data. The report is also intended to influence new development and future revisions of data systems, databases, and reporting requirements of related state agencies and programs.

The report summarizes the first phase of work of the California Interagency Data Collaboration (CIDC). The ultimate purpose of the CIDC is to improve the efficiency and quality of integrated children's and family services provided in California. To support this goal, the direct objectives of the collaboration are:

- *to reduce the data collection burden on case managers at local Healthy Start sites and other similar interagency collaborations; and*
- *to facilitate the local use of data which must be collected to meet non-local mandates.*

These objectives have been addressed through the consensus development of three types of standards:

- ***data translation standards** for sharing core data elements among local agencies, and between local and state agencies;*
- ***functional specification standards** for local case management information systems; and*
- ***confidentiality standards** related to sharing client data between agencies.*

These are the standards presented in this report, as described below.

CORE DATA ELEMENTS

Section II includes a directory of the three levels of core data elements selected for development of data translation standards. Detailed definitions and coding structures are provided for Levels 1 and 2 elements, together with initial mapping to the national and California student transcript data standards (*ANSI SPEEDE/ExPRESS Transaction Set 130* and the *California Student Information Services (CSIS) Student Data Handbook*, draft version). Definitions are not yet available for Level 3 elements. Additional work on selection of data elements for Level 3, together with development of definitions and structures for the Level 3 data elements, should be part of any future work of the collaboration.

These standards are intended for use as a common data translation language across programs and agencies. Use of these standards for data representation within local or state databases is optional and not required for participation in data exchange. However, to effectively participate an agency's data must be collected in a manner which is translatable to and from these standards with minimal loss of information.

All data names, definitions, and coding structures are designed to be maximally compatible with ANSI TS-130 and CSIS. Where our local interagency data sharing needs differ or go beyond those addressed in these systems, we intend to apply for changes and work with these groups to ultimately reach the goal of full compatibility across systems.

Level 1: Core Linkage Data

This minimal set of data elements was selected to provide the greatest likelihood of successful matches of individuals across databases. It contains the following elements:

- Client Name
- Date of Birth
- Gender
- County of Birth
- State of Birth
- Country of Birth
- Reference Number
- Reference Number Type
- Mother's Name
- Mother's Maiden Name

Level 2: Minimal and Essential Case Management Data

These elements were selected as the smallest subset of data which should readily be available to a case manager for a new client who has already completed an intake for another program. The following elements are included for (1) *the client*, (2) *the primary contact*, (3) *one or more other parents or guardians*, and (4) *one or more other family members*:

- Name
- Date of Birth
- Gender
- Reference Number
- Reference Number Type

- Marital Status
- Lives in Household
- Street Address, City, State, Zip Code, and Telephone Number
- English Proficiency
- Preferred Language

Also included for *the client* only are:

- Interpreter Flag
- Race/Ethnicity

And for each *family member*:

- Relationship to Client

Level 3: Other Core Case Management Data for Sharing

These are data considered optional for sharing, and consist of the CISLS evaluation data together with other important data elements which potentially might be shared across some programs. Initial priority elements have been selected so far in the following categories (please see Section II of the report for the complete listing):

- Education
- Health
- Household Information
- Risk Indicators
- Service Referrals and Encounters
- Pregnancy Outcomes

CMIS FUNCTIONAL SPECIFICATIONS

Section III contains 43 standards for case management information system (CMIS) functional specifications. These standards are intended to apply to several situations, including modifying an existing system, evaluating and purchasing a new system, or working with a vendor or in-house data systems staff to design and develop a CMIS unique to the user.

The 43 standards are organized into seven functional categories:

- *System functionality* describes the functions required of a CMIS to satisfy the information management needs of a comprehensive integrated school-linked service program.

- *System design* describes the capabilities to be met by the configuration of hardware and software employed, independent of the particular computer or operating system.
- *User interface* describes system features which facilitate and enhance the users' interaction with the computer system, such as data entry, menu choices and system help.
- *System security* provides standards for protecting records from inadvertent or intentional disclosure, unauthorized access, and loss.
- *Management reports* identifies important system generated reports for case management and resource planning.
- *Interconnectivity* describes capabilities for importing and exporting data from external systems, automating eligibility determination, and assisting case managers in annotating case records.
- *Vendor services, agreements and training* presents standards for ensuring a happy and ongoing relationship between agency and vendor.

Each of the 43 standards presented in Section III has been classified into one of three categories: *primary, secondary* or *conditional*. Primary standards are those that should be met by all systems, unless a sound professional reason is available to show why it is not necessary or technically feasible to do so in a particular case. Secondary standards are desired as goals, but likely to be beyond reasonable expectations in some situations. Conditional standards are those which vary with the application, and may be either primary or secondary depending on the situation.

Explanatory comments, examples and cross-references are provided to assist the user, regardless of computer experience, in understanding and applying the standards.

CONFIDENTIALITY

While data sharing between agencies usually increases the efficiency of serving clients and can lead to better, more comprehensive case management, it also poses potential threats to client privacy. Service providers must keep in mind that their clients are being asked to provide information that is often sensitive, personal and private. The final section of this report presents standards for protecting the confidentiality of client information in the course of interagency data sharing. It aims to strike a balance between the needs of clients for privacy and the needs of agencies for client information.

This section discusses the importance of protecting the privacy of children and families, and presents 23 standards for protecting the confidentiality of client data. The standards are organized into the four categories of: (1) *basic principles*, (2) *permissible disclosures*, (3) *procedures to protect confidentiality*, and (4) *automated systems*. Each standard should be considered "primary"; it is essential that every participating agency and program adhere to each standard in order to fully safeguard client confidentiality. These standards include four major principles which serve to ensure that confidential client information is disclosed only when necessary, thereby limiting the potential harm that can result from sharing sensitive client data:

- Agencies should presume that client information and records are confidential and should not disclose client data unless a specific exception to the presumption of confidentiality applies or the disclosure is authorized by the client, a court or another appropriate mechanism.
- An interagency collaborative effort should satisfy the strictest legal and professional standards for confidentiality owed by any participating agency.
- Agencies should collect and record only that information that is genuinely needed to fulfill the goal of serving the client. This principle suggests that agencies can minimize the potential of harming clients through improperly disclosing personal data by maintaining or sharing only the minimal necessary information.
- At the initial meeting with each client, or soon after, agency personnel should conduct a thorough and meaningful discussion with the client about the agency's practices with regard to confidential information. Clients who understand how information about them will be maintained and used are more likely to seek services and allow their information to be shared with other agencies.

Also provided (in Appendices B and C) are charts of federal and California confidentiality statutes and regulations. These charts contain detailed information on all federal and California statutes and regulations pertaining to the handling of confidential information about children and families. The charts are intended to assist school-linked services collaborations, as well as other interagency collaborations, in developing memoranda of understanding and interagency agreements regarding sharing client data.

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

TABLE OF CONTENTS vi

INDEX TO CASE MANAGEMENT INFORMATION SYSTEMS FUNCTIONAL SPECIFICATIONS STANDARDS viii

INDEX TO CONFIDENTIALITY STANDARDS FOR DATA SHARING AND CASE MANAGEMENT INFORMATION SYSTEMS xi

PREFACE xiii

SECTION I: INTRODUCTION 1.1

Policy and Program Context 1.1
The Problem 1.1
Data Sharing 1.1
Management Information Systems 1.2
Objectives of the Collaboration 1.2
Intended Applications of the Standards 1.2
Planning for Local Implementation 1.3
Levels of Data Addressed 1.4
Applicable Data Exchange Models 1.5
Likely Data Exchange Situations 1.5
Data Exchange Models Matrix 1.6
Categories of Standards 1.7
Cautions to be Exercised in the Use of these Standards 1.8
Organization of this Document 1.8
Glossary of Acronyms and Abbreviations Found in this Report 1.10

SECTION II: CORE DATA ELEMENTS DIRECTORY AND DEFINITIONS 2.1

Levels of Data 2.1
How to Use this Section 2.2
Data Flower 2.3
Databases and Data Systems 2.4

Core Data Elements Directory 2.5
Level 1: Core Linkage Data Elements Definitions and Codes 2.9
Level 2: Minimal and Essential Core Case Management
Data Elements Definitions and Codes 2.20
Data Element Qualifiers Definitions and Codes 2.45

SECTION III: CASE MANAGEMENT INFORMATION SYSTEMS FUNCTIONAL SPECIFICATION STANDARDS 3.1

System Functionality 3.1
System Design 3.5
User Interface 3.10
System Security 3.13
Management Reports 3.15
Interconnectivity 3.17
Vendor Services, Agreements, and Training 3.18

SECTION IV: CONFIDENTIALITY STANDARDS FOR DATA SHARING AND CASE MANAGEMENT INFORMATION SYSTEMS 4.1

How to Use these Standards 4.3
Basic Principles 4.4
Permissible Disclosures 4.6
Procedures to Protect Confidentiality 4.11
Automated Systems 4.16

APPENDICES

APPENDIX A CSIS Race/Ethnicity Codes
APPENDIX B Federal Confidentiality Statutes and Regulations
APPENDIX C California Confidentiality Statutes and Regulations

REFERENCES

INDEX TO CASE MANAGEMENT INFORMATION SYSTEMS FUNCTIONAL SPECIFICATIONS STANDARDS

SYSTEM FUNCTIONALITY Page

Standard 3.1: Family-Oriented Record 3.1

Standard 3.2: Chronological Tracking 3.2

Standard 3.3: Appointment Scheduler/Tickler System 3.3

Standard 3.4: Pre-Printed Form Generation 3.3

Standard 3.5: Support for Third Party Reimbursement 3.4

Standard 3.6: Back-Up and Recovery Systems 3.4

Standard 3.7: User System Modification 3.4

Standard 3.8: Archiving Data 3.5

SYSTEM DESIGN

Standard 3.9: Single- and Multi-User Environments 3.5

Standard 3.10: Automated File and Record Locking 3.6

Standard 3.11: Open File Structure 3.6

Standard 3.12: Modular System Design 3.7

Standard 3.13: Core Linkage Data and Client Search Algorithm 3.7

Standard 3.14: Core Data Elements and Standard Definitions 3.7

Standard 3.15: Minimized Redundant Data Entry 3.7

Standard 3.16: Data Range Checking 3.8

Standard 3.17: Conditional Skipping of Fields 3.8

Standard 3.18: Required Data Fields 3.9

Standard 3.19: Attached Laser Printer 3.9

Standard 3.20: Multiple Printer Output 3.9

Standard 3.21: Print Spooling 3.9

Standard 3.22: SQL Interface 3.10

USER INTERFACE

Standard 3.23: Consistent Commands 3.11

Standard 3.24: Status Communication 3.11

Standard 3.25: Menus or Decision Trees 3.11

Standard 3.26: On-Line Help 3.11

Standard 3.27: Changing Help Messages 3.12

Standard 3.28: Function Keys 3.12

Standard 3.29: Alternate Data Entry Devices 3.12

SYSTEM SECURITY

Standard 3.30: Password Protection 3.13

Standard 3.31: Multiple Levels of Security 3.13

Standard 3.32: On-Line Security Control 3.14

Standard 3.33: Automatic Screen Blanking/Lockout 3.14

Standard 3.34: Modem Dial Back 3.14

Standard 3.35: Locked System Servers and Terminals 3.15

MANAGEMENT REPORTS

Standard 3.36: Standard Reports 3.15

Standard 3.37: Ad Hoc Reports 3.16

INTERCONNECTIVITY

Standard 3.38: Data Import and Export 3.17

Standard 3.39: Automatic Determination of Program Eligibility 3.17

Standard 3.40: E-Mail, Editor and Report Writer 3.17

VENDOR SERVICES, AGREEMENTS, AND TRAINING

Standard 3.41: Standard Software Characteristics 3.18

Standard 3.42: Written Guarantee of Limited Cost-Free Repair 3.19

Standard 3.43: Other Written Agreements 3.19

INDEX TO CONFIDENTIALITY STANDARDS FOR DATA SHARING AND CASE MANAGEMENT INFORMATION SYSTEMS

BASIC PRINCIPLES Page

Standard 4.1: Presumption of Confidentiality 4.4

Standard 4.2: Satisfy the Strictest Standard Required 4.4

Standard 4.3: Collect Only Necessary Information 4.5

Standard 4.4: Informing Clients 4.6

PERMISSIBLE DISCLOSURES

Standard 4.5: Sharing "Non-identifiable" Information 4.6

Standard 4.6: Sharing Non-confidential Personal Information 4.7

Standard 4.7: Intra-agency Information Sharing for Administrative Purposes 4.7

Standard 4.8: Mandatory Disclosure in Limited Circumstances 4.8

Standard 4.9: Client Consent 4.8

Standard 4.10: Obtaining Informed Consent 4.8

Standard 4.11: Consent of Minors to Release Information 4.9

Standard 4.12: Requirements of Consent 4.10

Standard 4.13: Court Orders 4.11

Standard 4.14: Client Access to Records 4.11

PROCEDURES TO PROTECT CONFIDENTIALITY

Standard 4.15: Staff Training 4.11

Standard 4.16: Response to Requests for Information 4.12

Standard 4.17: Designated Staff Person: "Gatekeeper" 4.13

Standard 4.18: Confidentiality Oaths 4.13

Standard 4.19: Written Agreements Among Agencies 4.14

Standard 4.20: Referrals Among Agencies 4.15

Standard 4.21: Documentation of Disclosure 4.15

AUTOMATED SYSTEMS

Standard 4.22: Computerized Information 4.16

Standard 4.23: Security Procedures for Automated Systems 4.17

PREFACE

The California Interagency Data Collaboration (CIDC) was proposed by a group of California state and local agency representatives and other children's services participants convened by the Stuart Foundations between December, 1992 and March, 1993. Far West Laboratory for Educational Research and Development (FWL) was designated as the contractor and the project began in late April, 1993 upon funding by the Foundation Consortium for School-Linked Services in partnership with the California Departments of Education and Health Services.

The objectives of the collaboration are to (1) reduce the data collection burden on case managers at local Healthy Start sites and other similar interagency collaborations; and (2) facilitate local use of data which must be collected to meet non-local mandates. These two objectives are addressed through the consensus development of standards and procedures for data sharing and data transmission, functional specification standards for local case management information systems (CMIS), and confidentiality standards for the exchange of client data among agencies.

The CIDC has involved broad participation across relevant state and local public agencies, local Healthy Start sites, and software vendors. Much of the collaboration's work has been accomplished with contributed staff time from these groups and individuals. The technical work and standards development activities were performed by CIDC technical advisory group members working in four task groups during the past year (Core Data Elements, Data Sharing Methodology, MIS Functional Specifications, and Confidentiality). Additional input came from CISLS site staff and evaluation coaches and software vendors who participated in meetings, site visits, panel discussions, surveys, and phone conversations. All CIDC participants (see list below) received the Version 1 draft of this report and had the opportunity to provide comments and suggestions. All sixty-five of the CISLS operational sites also were solicited for comments.

The publication of this document (Version 2.0) marks the completion of the first phase of the CIDC. At the time of this writing, no funding for further work of the collaboration has been allocated. It is anticipated, however, that future work eventually will be funded to build on the foundation established in Phase I.

PROJECT STAFF AND COMMITTEE MEMBERS

Project Staff

Norm Constantine, Project Director, *Far West Laboratory*
Julie Aronson, Research Associate, *Far West Laboratory*
Berlina Ceguerra, Office Assistant, *Far West Laboratory*
Ann Wallgren, Administrative Assistant, *Far West Laboratory*

Steering Committee

George (Peter) Abbott, *California Department of Health Services*
Dion Aroner, *Assembly Human Services Committee*
Lin Barrett, *Marin County Coordinated Youth Services Council*
Judy Chynoweth, *Foundation Consortium for School Linked Services*
John DiCecco, *Los Angeles Unified School District*
Elaine Duxbury, *California Youth Authority*
Gary Feldman, *Ventura County Public Health Department*
Jane Henderson, *California Department of Education*
Ed Hernandez, *San Francisco County Department of Public Health*
Dale S. Holmes, *Riverside County Office of Education*
Julie Jackson, *California Department of Developmental Services*
Pat Jordan, *San Mateo County Mental Health Division*
Ann Louise Kuhns, *Health and Welfare Agency*
Amelia Loomis, *Stuart Foundations*
David Mitchell, *California Department of Health Services*
Tameron Mitchell, *California Department of Health Services*
Carmen Ochoa, *California Department of Economic Opportunity*
Bill Padia, *California Department of Education*
Stephen Rhoads, *California Office of Child Development and Education*
Jeannemarie Solak, *California Department of Education*
Elizabeth Varney, *Siskiyou County Welfare Department*
John Webb, *California Department of Social Services*

Technical Advisory Group

Kathleen Alarid-Barfield, *Far West Laboratory*
Thomas Bakke, *California Department of Developmental Services*
David Bell, *Family Health Outcomes Project, UCSF*
Eric Boutwell, *San Francisco Unified School District*
Alyson Boyle, *California Department of Economic Opportunity*
Mark Branagh, *Independent Consultant*

Ed Briles, *California Department of Health Services*
Claire Brindis, *UCSF Center for Reproductive Health Policy Research*
Sally Brown, *Independent Consultant*
Connie Busse, *New Beginnings Program*
Gwendolyn Doebbert, *California Department of Health Services*
Diane Enkoji, *Office of Information Technology*
Beth Hart, *Healthy Start Field Office*
Chris Haynes, *Independent Consultant*
David Kaplan, *Children's Hospital, Denver*
Sean Kirkpatrick, *Sean R. Kirkpatrick Consulting*
Elizabeth Mandell, *Lodestar Management/Research, Inc.*
Jane McCann Walsh, *Western Consortium for Public Health*
Walter McDonald, *Walter R. McDonald Associates, Inc.*
David Mitchell, *California Department of Health Services*
Ken Moody, *Health and Welfare Agency Data Center*
Geraldine Oliva, *Family Health Outcomes Project, UCSF*
Alan Oppenheim, *California Department of Health Services*
Clark Peters, *Youth Law Center*
Maria Ramiu, *Youth Law Center*
Lalit Roy, *California Department of Education*
Georgia Sales, *INFO LINE*
Janice Schafer, *Far West Laboratory*
Marie Schelling, *California Department of Economic Opportunity*
Werner Schink, *California Department of Social Services*
Roger Smith, *California Department of Health Services*
Mark Soler, *Youth Law Center*
Susan Starbuck-Morales, *UCSF Center for Reproductive Health Policy Research*
Kathy Styc, *California Department of Mental Health*
Bill Swift, *Marin County Coordinated Youth Services Council*
Lisa Villarreal, *San Mateo County Office of Education*
Lois Wainstock, *ACCESS MCH*
Mary Wagner, *SRI International*
Shannan Wilber, *Youth Law Center*

Healthy Start Site Panel and Reviewers

Lin Barrett, *Marin County Coordinated Youth Services Council*
Connie Busse, *New Beginnings Program*
Charlene Clemens, *San Francisco Teenage Pregnancy and Parenting Program*
Kyle Fiore, *St. John's Educational Threshold Center*
Carol Forest, *Daly City Youth Health Center*
Carolyn Getridge, *Alameda County Office of Education/Oakland Unified Consortium*

Frida Goldstein-Friend, *Santa Paula Elementary School District*
David Hastings, *Shoreline Unified School District*
Rhoda Katz, *UC Berkeley Children & Youth Policy Project*
Janet Reed, *Pajaro Valley Unified School District*
Ann Turner-Scott, *Howe Avenue School*

Management Information System Vendor Reviewers

Robert Alexander, *Sean R. Kirkpatrick Consulting*
Sean Kirkpatrick, *Sean R. Kirkpatrick Consulting*
Elizabeth Mandell, *Lodestar Management/Research, Inc.*
Walter McDonald, *Walter R. McDonald Associates, Inc.*
Georgia Sales, *INFO LINE*

PRIMARY CONTRIBUTORS TO THIS REPORT

This report was prepared by *Norm Constantine, Julie Aronson,* and *Shannan Wilber*, with significant writing and editing support from *Thomas Bakke, Mark Branagh, Ed Hernandez, Walter McDonald, Elizabeth Mandell,* and *Clark Peters.*

Other primary contributors through their work on the task groups were: *Kathleen Alarid-Barfield, Lin Barrett, David Bell, Connie Busse, Diane Enkoji, Amelia Loomis, Jane McCann Walsh, David Mitchell, Ken Moody, Geraldine Oliva, Maria Ramiu, Roger Smith, Janice Schafer*, and *Mark Soler.*

ACKNOWLEDGEMENT OF PREVIOUS WORK

This document builds on the important work completed prior to the start of the California Interagency Data Collaboration by the ANSI SPEEDE/ExPRESS groups, the California Student Information Services, the Family Health Outcomes Project, and the Youth Law Center. We are grateful for the solid foundation this work has provided.

RECOMMENDED NEXT STEPS

At the time of publication of this document, no funding has been allocated for any further work of the collaboration. The following recommendations for maintenance and support activities are contingent upon eventual restoration of funding.

Document Evolution

The current version of this report, Version 2.0, is based on consideration of comments and suggestions from the field and the CIDC steering committee in response to the December 8, 1993 field review draft document (Version 1.0). The next update of this document (Version 3.0) should include at least:

- the addition of the Level 3 core data elements definitions and coding structures, which include the CISLS evaluation data elements collected at all Healthy Start sites; and
- additional mapping to other program-specific data sets.

At the present time the CMIS functional specification standards and the confidentiality standards can be considered complete, subject of course to new additions and modifications which will derive from experiences in the field as sites and vendors attempt implementation. Version 3.0 of this document should incorporate modifications based on these experiences.

User Orientation and Support

The value of these standards will be greatly enhanced if regional orientation sessions for CISLS site staff are funded and presented. These sessions should provide guidance to site coordinators and on-site CMIS staff on using the standards to evaluate, select or design local integrated CMIS, and to develop data sharing procedures across agencies within sites. In addition, phone consultation should be made available on the same issues.

As CMIS vendors begin to develop or modify their systems to meet some or all of the standards, the collaboration should begin the process of describing each system and rating its compliance with the standards for publication. A statewide orientation session also should be held for software vendors to explain the standards and the process to be used for summarizing and rating systems. Additional phone consultation should be made available to vendors who attempt to implement the standards.

SECTION I: INTRODUCTION

This report provides standards and procedures intended to serve as tools to local comprehensive integrated school-linked services (CISLS) sites and software vendors which are developing and implementing case management information systems for the management and exchange of client data. The report is also intended to influence new development and future revisions of data systems, databases, and reporting requirements of related state agencies and programs.

POLICY AND PROGRAM CONTEXT

The Problem

In California, as in many other states, there has been a trend away from specific, categorically-funded service delivery in favor of more comprehensive, integrated, school-linked services. Integrated services programs bring together the services traditionally provided in isolation by public and private agencies of health, education, social services, and mental health to promote the overall well being of children and families.

As children's services in California become integrated, the need increases both for (1) data sharing across programs, and (2) integrated management information systems to facilitate serving and tracking clients across programs. Unfortunately, the present reality falls short in meeting either of these needs, thereby increasing the burden on site staff and clients and potentially compromising both the quantity and quality of services provided.

Data Sharing

Local sites moving forward with service integration inevitably run into the barrier of data requirements and data systems across categorical programs which are incompatible and insufficiently flexible to function efficiently in an integrated services environment. Clients who are served by more than one program are often subject to answering similar or redundant intake and follow up questions. This is because mechanisms for transfer of data from system to system usually do not exist, and more fundamentally due to the incompatibility of data definitions, data coding structures, and data collection procedures for many data elements across programs. Even when the data need not be collected redundantly from clients, program staff are burdened with filling out redundant forms and entering redundant data into different systems. Many of these systems *individually* require extensive data collection and management; when the *multiplicative burden* to clients and local staff across systems is examined, the immediate need for more efficient data sharing becomes clear.

Management Information Systems

The other need which expands as services become integrated is the requirement for increased support from case management information systems in serving and tracking clients across programs. The CISLS evaluation provides each site with a data entry screen to create a data file of site-entered data for transmission to the evaluation office. No on-site management information reports, however, are included in the scope of this system. As a result, many CISLS sites are poised to invest in development of these systems locally. If data sharing and system design specifications are not standardized, both duplication of effort and divergence of systems will result.

Objectives of the Collaboration

The ultimate purpose of the CIDC is to improve the efficiency and quality of integrated children's and family services provided in California. To support this goal, the direct objectives of the collaboration are:

- *to reduce the data collection burden on case managers at local Healthy Start sites and other similar interagency collaborations; and*
- *to facilitate the local use of data which must be collected to meet non-local mandates.*

These objectives have been addressed through the consensus development of three types of standards:

- ***data translation standards** for sharing core data elements among local agencies, and between local and state agencies;*
- ***functional specification standards** for local case management information systems; and*
- ***confidentiality standards** related to sharing client data between agencies.*

These standards are presented in the following three sections of this report.

Intended Applications of the Standards

The standards in this document are addressed to local program sites providing comprehensive school-linked children's and family services consistent with the definition of a CISLS (Healthy Start/SB 620) site. However, application is not limited to currently funded CISLS sites. Any program which is based on a collaboration among service agencies, is family focused and case management oriented, and collects evaluation data should benefit. In addition, these standards are for the use of any state agency or program which has at least one local implementation involved in a CISLS or other interagency collaboration as defined above.

It is the policy of the CIDC that no attempt is made to impose data definitions or coding structures on any agency's data base or system, local, state, or otherwise. Rather, through the consensus process of developing the core data elements standards, we have attempted to generate a *common translation language* for exchange of data between local collaborative partners, and between local and state agencies. This approach is consistent with the widely employed electronic data interchange (EDI) model, which is the basis of many tested and successful data exchange systems, including the national and California systems for electronic exchange of student records (ANSI TS-130 and CSIS). The EDI model provides for one common set of data definitions and coding structures to be used in all data transmissions between trading partners. Where previously each agency would have to perform as many translations as it had trading partners, a common EDI set of standards allows each agency to support only one translation and yet be able to exchange data with all other participating agencies. No attempt is made to impose standards on an agency's own data base; however, to participate in data exchange the agency's data must be collected and stored in a manner which is translatable to and from the core data elements standards with minimal loss of information.

The collaboration's intent with the CMIS functional specifications standards and the confidentiality standards is to make available to local sites and software vendors the benefit of our consensus work, thereby providing the sites and vendors with a significant head start in designing and implementing their systems. These standards are intended to facilitate informed decisions and to save work, as well as ultimately to encourage more responsive and responsible systems with maximum consistency across sites.

Planning for Local Implementation

It is important to recognize that local site implementation of a data sharing relationship and/or a CMIS will occur differently, depending upon the experiences, needs, and resources of the participating organizations. The standards in this document will need to be tailored to the to the specific context of the local collaboration.

How the standards are implemented partly will depend on who participates in the planning process. Therefore one of the most important initial tasks is to bring together all stakeholders in the local integrated services collaboration for a discussion of data system needs. When it is determined which agencies will participate in data sharing, a steering committee should be formed to develop objectives for the data system and data sharing, define the scope of implementation, identify and prioritize goals, and determine resources available. In addition, a technical advisory committee should be appointed to define the technical features of the proposed data system, review relevant existing systems, conduct a feasibility study if necessary, specify means of selecting a contractor, and maintain ongoing communication with the contractor. It is not always necessary to develop new systems. This group should have the expertise to determine whether a new CMIS should be developed or if an existing system can be modified appropriately.

Every effort should be made to procure a CMIS that is both easy and efficient to use. Likewise, the system should minimize the need for highly technical personnel, such as programmers. To accomplish these objectives, special emphasis should be placed on training and documentation, both of which can be done on-line (e.g., tutorials and help screens) and off-line (e.g., group training and published materials). In some cases, however, the more complicated systems may require that a system operator be retained on at least a part-time basis.

The more complex the proposed CMIS, either in number of participating agencies or in technical features, the more important and time consuming these tasks will be. Taking the appropriate time to consider all options thoroughly will pay off in the end. Communities with limited resources are especially encouraged to review existing CMIS developed for similar purposes by other communities with similar needs and characteristics.

Levels of Data Addressed

The figure which appears in the introduction to Section II shows a data flower representation of the levels of data found across many of the service programs available in California. The inner circle of the flower represents the *Level 1, core linkage data elements*. This minimal set of data elements was selected by the core data elements task group to provide the greatest likelihood of successful matches of individuals across databases. The next concentric circle represents the *Level 2, minimal and essential core case management data elements*. These elements were selected as the smallest subset of data which should readily be available to a case manager for a new client who has already completed an intake for another program. The outermost concentric circle represents *Level 3, other core case management data elements.* These are data considered optional for sharing, and consist of the CISLS evaluation data together with other important data elements which might potentially be shared across some programs.

Applicable Data Exchange Models

Six basic models of data exchange were identified by the data sharing methodology task group. In reality, at any particular CISLS site a combination of two or more of these models might be implemented simultaneously:

1. *fully integrated CMIS across multiple service programs;*
2. *computerized data exchange based on on-line access to other systems;*
3. *computerized data exchange based on batch requests and responses;*
4. *computerized data exchange based on regularly scheduled import and export of data for entire potential client base;*
5. *data exchange based on paper forms; and*
6. *data exchange based on voice communication.*

The table below represents the task group's preliminary attempt to analyze these six models in terms of the major model elements. Additional work is needed on the implications of particular data exchange models to the application of these standards, and on development of additional standards related to other important data exchange methodology issues including data discrepancy resolution, data updating and purging, and data directories design.

Of the standards in this report, the core data element definitions apply equally across all six models, while the CMIS functional specifications standards apply most to the first model, and to a lesser extent to the second through fourth models. The confidentiality and security standards vary in their applicability by standard, but most of these standards apply to all or most of the data exchange models.

Likely Data Exchange Situations

Many of the considerations related to data sharing methodology depend on the range of programs across which the data are shared. The range of programs for data sharing can be categorized into three levels: data can be shared among programs which are partners of a collaborative, between programs within the same geographical/ political area (such as a county or school district) but which are not part of a collaborative, and between same-type programs across geographical/political boundaries. These standards are intended to address all three situations, although the CMIS functional specification standards are primarily applicable to the first situation (partners within a collaborative).

DATA EXCHANGE MODELS MATRIX

MAJOR MODEL ELEMENTS

BASIC DATA EXCHANGE MODELS	Data Integration (none, partial, full)	Data Form (not recorded, paper, electronic)	Exchange Media (voice, paper, removable magnectic, electronic)	Data Location (central, distributed)	Data Currency (real time, point-in-time)	Data Availability (immediate, delayed)	Data Ownership (single, multiple)	Transmission Reliability (high, medium, low)	Transmission Security (high, medium, low)	System Expandability (easy, moderate, difficult, impossible)
Fully integrated computerized multi-program system.	full	electronic	electronic	either	real time	immediate	multiple	high	high	moderate
Computerized data exchange based on on-line access to other data systems.	partial	electronic	electronic	distributed	real time	immediate	single	high	moderate	moderate
Computerized data exchange based on batch requests and responses.	partial	electronic	magnetic	distributed	point-in-time	delayed	single	high	moderate	moderate
Computerized data exchange based on regularly scheduled export/import of data for entire potential client base.	partial	electronic	magnetic	distributed	point-in-time	delayed	single	high	high	moderate
Data exchange based on paper forms.	partial, none	paper	paper	either	point-in-time	delayed	single	low	low	easy
Data exchange based on voice communication	partial, none	not recorded	voice	distributed	real time	immediate	single	medium	medium	easy

BEST COPY AVAILABLE

1. Collaborative partners

The need for sharing data across collaborative partners is the most typical CISLS situation. One advantage is that written agreements and memoranda of understanding (MOU) will be place between the partners, potentially simplifying the confidentiality and procedural issues. While any of the six basic data exchange models might be applicable here, this is the only situation where Model 1, a fully integrated multi-program system, would apply.

2. Non-partners within same geographic or political unit

Often an agency sees a family which has previously been seen by a different agency in the community that is not part of the collaborative. While this situation is not fully consistent with the CISLS model, in reality it is often encountered. It is unlikely that data exchange Models 1, 2, or 4 would apply here, while Model 3, batch request and response might apply, and Models 5 and 6, paper and voice exchange, would be most likely. Confidentiality issues are more difficult due to the lesser likelihood of written agreements or MOU between agencies being in place.

3. Same type programs outside of service area

A local agency might desire to obtain data from a family that has recently relocated to the service area and has had extensive service encounters in a previous county or location. This is the type of situation upon which the California Student Information System (CSIS) is based, and fits well with data exchange Model 3, batch requests and responses, the model employed by CSIS. Although it is possible to consider different program-type data transfers across geographical boundaries, the more likely need would be for same program type data, such as old school records to the new school, or previous social service data to the new social service agency. While site based written agreements or MOU are not likely to be in place here, existing intra-agency policies or agreements might partially address confidentiality concerns.

CATEGORIES OF STANDARDS

All standards have been or will be classified into one of the following three categories. These categories were modeled after the *American Psychological Association's* test standards. They were developed to reflect the reality that not all desirable features are practical or possible in all situations, and that the importance of some standards might vary by situation.

Primary Standards: those that should be met by all systems, unless a sound professional reason is available to show why it is not necessary, or technically feasible, to do so in a particular case.

Secondary Standards: desired as goals, but likely to be beyond reasonable expectations in many situations.

Conditional Standards: the importance of the standard varies with the application, and may be either primary or secondary depending on the situation.

CAUTIONS TO BE EXERCISED IN THE USE OF THESE STANDARDS

The current report is Version 2.0 of a living, evolving document. Use of these standards during the first year after publication should be considered a field test. Over time the collaboration will learn from the experiences of the sites and vendors who try to implement these standards, as well as from the overall experiences of sites that are moving forward with their approaches to collaboration and implementing integrated services programs. We know that these standards initially will be incomplete, and that in spite of the massive reviews this document has undergone there exist in these standards bugs that will only be discovered upon application in particular real life situations. At the same time, we can expect regular changes in programs funded, programmatic approaches, state and federal mandates, and available technology, all potentially requiring changes in some parts of the standards to maintain their currency. It is the collaboration's intent that this version of the standards will be useful to local sites and software vendors as it is, and that future efforts will ensure continued improvement and currency in a manner minimally disruptive to all involved.

ORGANIZATION OF THIS DOCUMENT

Section I: Introduction discusses the purpose and intent of the standards, and the types of programs and situations to which they apply. This section also includes definitions of the three categories of standards: *primary*, *secondary*, and *conditional*.

Section II: Core Data Elements Directory and Definitions, includes the directory of elements selected for inclusion in the three levels of core data: *Level 1 (core linkage data)*, *Level 2 (minimal and essential core case management data)*, and *Level 3 (other core case management data)*. Definitions and coding structures are provided for Levels 1 and 2 elements, together with initial mapping to ANSI TS-130 and CSIS. Definitions and coding structures for the Level 3 data elements remain to be developed.

Section III: Case Management Information System Functional Specifications Standards, provides 43 design and functionality standards for case management information systems. These standards are intended both for the site staff who will be evaluating or locally designing a CMIS, and for vendors and other CMIS developers who will be modifying or designing systems.

Section IV: Confidentiality Standards for Data Sharing and Case Management Information Systems provides 23 standards related to confidentiality and issues in sharing data across programs. In addition, Appendices B and C include charts of federal and California statutes and regulations pertaining to the sharing of client data.

GLOSSARY OF ACRONYMS AND ABBREVIATIONS FOUND IN THIS REPORT

AFLP	Adolescent Family Life Program (DHS)
ANSI	American National Standards Institute
ANSI TS-130	American National Standards Institute - Transaction Set 130. This transaction set contains the data that would be found in an electronic student transcript as developed by the SPEEDE and ExPRESS work groups.
CASEMIS	California Special Education Management Information System (CDE)
CBEDS	California Basic Education Data System (CDE)
CDE	California Department of Education
CDS	Client Data System (DMH)
CHDP	California Health and Disability Prevention System (DHS)
CIDC	California Interagency Data Collaboration
CISLS	Comprehensive Integrated School-Linked Services
CMIS	Case Management Information System
CMIS	Client Management Information System (DDS)
CSIS	California Student Information Services (CDE)
CWS/CMS	Child Welfare Services/Case Management System (DSS)
DDS	California Department of Developmental Services
DHS	California Department of Health Services
DMH	California Department of Mental Health
DSS	California Department of Social Services

EDI	Electronic Data Interchange
ExPRESS	Committee on the Exchange of Permanent Records Electronically for Students and Schools
FHOP	Family Health Outcomes Project (DHS)
FWL	Far West Laboratory
GAIN	Greater Avenues for Independence (DSS)
GUI	Graphical User Interface
INS	Immigration and Naturalization Service
JTPA	Job Training Partnership Act
MEDS	Medi-Cal Eligibility Data System (DHS)
MIS	Management Informations System
MOU	Memorandum/Memoranda of Understanding
SANDIS	San Diego Information System (DDS)
SB 620	Healthy Start Support Services for Children Act (1991)
SPEEDE	Standardization of Postsecondary Education Electronic Data Exchange
SQL	Structured Query Language
SRI	Stanford Research Institute
SSN	Social Security Number

SECTION II: CORE DATA ELEMENTS DIRECTORY AND DEFINITIONS

This section presents data translation standards for sharing core data elements among local agencies, or between local and state agencies. The standards consist of common data element definitions and coding structures, and are intended for use as a data translation language across programs and agencies. Use of these standards for data representation within local or state databases is optional and not required for participation in data exchange. However, to effectively participate an agency's data must be collected in a manner which is translatable to and from these standards with minimal loss of information.

LEVELS OF DATA

The data flower diagram in Figure 1 represents the levels of data found across many of the databases and data systems used by California agencies and programs. The three concentric circles within the flower represent the core data, or those data elements with the highest potential for effective sharing. The petals of the flower represent non-core, program-specific data elements, those which are required by specific programs or agencies but are not as likely to be shared across programs or agencies.

The innermost circle of the flower represents the ***Level 1, Core Linkage Data***. This minimal set includes those data elements which provide client identifying information least likely to change over time, thereby providing the greatest likelihood of successful matches of individuals across distinct databases.

The next concentric circle represents the ***Level 2, Minimal and Essential Core Case Management Data***. These elements comprise the smallest subset of data which provide client information that most agencies are likely to require, and potentially share. These are the data which should be readily available to a case manager for a new client who has already completed an intake for another program. Basic family member information has been included at this level, reflecting the focus on family-centered service programs.

Levels 1 and 2 data elements and coding structures have been reviewed widely and agreed on by the various collaboration committees. If data sharing is to take place, all available Levels 1 and 2 data elements should be included in the exchange.

The third concentric circle represents ***Level 3, Other Core Case Management Data***. These are case management data often collected by service agencies but considered optional for sharing with any specific trading partner. These data will consist of the CISLS evaluation data, as well as other important health and human services data elements. These elements are included as core data because developing standards for these elements will allow agencies to more readily share data when they elect to do so. Again, the exchange of these data are optional and highly dependent on the specific situation.

Preliminary selection of Level 3 data elements has been completed by the core data elements task group. The selection of additional elements and the development of coding structures for all Level 3 elements remain to be completed. Work completed to date also has included the analytic mapping between the CISLS evaluation data service categories and definitions to the comparable INFO LINE Taxonomy of Human Services categories and definitions.

Program-specific data, represented by the flower petals in Figure 1, are not as likely candidates for sharing across agencies. These data have not been addressed in the standards development effort.

HOW TO USE THIS SECTION

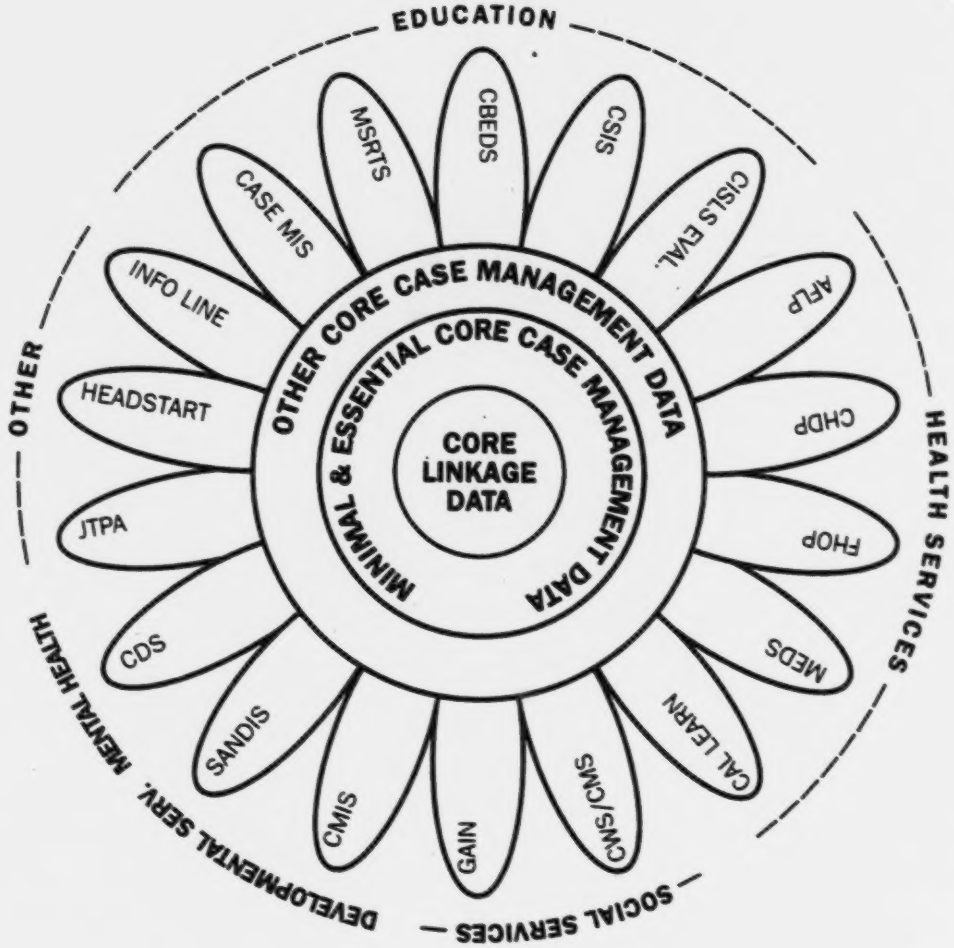
This section includes all of the core data elements selected for inclusion in Levels 1, 2, and 3. For Levels 1 and 2 elements only, definitions and coding structures are provided, together with mapping to the *ANSI SPEEDE/ExPRESS Transaction Set 130* and the *California Student Information Services (CSIS) Student Data Handbook* (draft version).

The *Core Data Elements Directory* provides the core data elements grouped by level and listed in the order in which they appear in the detailed technical descriptions which follow the directory. In the directory, data elements are positioned to reflect their relationship to one another. For example, demographic data elements indented under *Client* reflect that those data elements refer to that client. Data elements which may appear more than once in a record are marked *repeatable*.

All data element names, definitions, and coding structures have been designed to be maximally compatible with ANSI TS-130 and CSIS. At the bottom of each technical description page are listed those data elements in ANSI and CSIS that most closely correspond to the data element described. In some cases, new data elements and/or coding options have been created for existing ANSI or CSIS data elements. Where our local interagency data sharing needs differ or go beyond those addressed by ANSI, CSIS, or other systems, changes will be requested in these systems, and it is expected that all groups will work together to ultimately reach the goal of maximum compatibility across systems.

Where possible, we have included full ANSI or CSIS codes with the data element definition, or, where the list was extensive, we have referred the reader to an appendix. In other cases, where the list was very long and overly specific (e.g., zip codes), we have referenced the appropriate ANSI TS130 appendix but have not included the list in this document.

FIGURE 1.
DATA FLOWER


EDUCATION
MSRTS
CBEDS
CSIS
CISLS EVAL.
CASE MIS
INFO LINE
AFLP
HEADSTART
CHDP
JTPA
FHOP
CDS
MEDS
SANDIS
CAL LEARN
CMIS
GAIN
CWS/CMS
OTHER
HEALTH SERVICES
MENTAL HEALTH
DEVELOPMENTAL SERV.
SOCIAL SERVICES
OTHER CORE CASE MANAGEMENT DATA
MINIMAL & ESSENTIAL CORE CASE MANAGEMENT DATA
CORE LINKAGE DATA

The labeled petals contain only a subset of existing and planned databases and data systems across the state. Please refer to the following page for a more comprehensive listing.

DATABASES AND DATA SYSTEMS

The following is a list of many of the state and local databases and data systems which either currently exist or are under development. While not an exhaustive list, it goes beyond what could be represented in the flower diagram in Figure 1.

California Department of Developmental Services (DDS)

CMIS	Client Management Information System
SANDIS	San Diego Information System

California Department of Education (CDE)

CASEMIS	California Special Education Management Information System
CBEDS	California Basic Education Data System
CSIS	California Student Information Services
MSRTS	Migrant Student Record Transfer System

California Department of Health Services (DHS)

AFLP	Adolescent Family Life Program
CHDP	California Health and Disability Prevention System
MEDS	Medi-Cal Eligibility Data System

California Department of Mental Health (DMH)

CDS	Client Data System

California Department of Social Services (DSS)

CWS/CMS	Child Welfare Services/Case Management System
GEMS	GAIN Management Information System
SAWS	Statewide Automated Welfare System

California Youth Authority (CYA)

OBITS	Offender-Based Informational Tracking System

Other Databases and Data Systems

ANSI - TS130	American National Standards Institute - Transaction Set 130 (Student Transcript Records)
CISLS (SRI)	Comprehensive Integrated School-Linked Services (Evaluation)
FHOP (UCSF)	Family Health Outcomes Project
JTPA	Job Training Partnership Act
SPEEDE/ExPRESS	Same as ANSI - TS130

CORE DATA ELEMENTS DIRECTORY

LEVEL 1: CORE LINKAGE DATA ELEMENTS (CL)

- **CL1** Client Name (*repeatable*)
  - **CL2** Date of Birth
  - **CL3** Gender
  - **CL4** County of Birth
  - **CL5** State of Birth
  - **CL6** Country of Birth
  - **CL7** Reference Number (*repeatable*)
    - **CL8** Reference Number Type
  - **CL9** Mother's Name
    - **CL10** Mother's Maiden Name

LEVEL 2: MINIMAL AND ESSENTIAL CORE CASE MANAGEMENT DATA ELEMENTS (ME)

- **ME1** Street Address (Client)
  - **ME2** City
  - **ME3** State
  - **ME4** Zip code
  - **ME5** Telephone Number (*repeatable*)
- **ME6** English Proficiency
- **ME7** Preferred Language
- **ME8** Interpreter Flag
- **ME9** Race/Ethnicity
- **ME10** Marital Status

- **ME11** Primary Contact Parent/Guardian Name
  - **ME12** Relationship to Client
  - **ME13** Date of Birth
  - **ME14** Gender
  - **ME15** Reference Number (*repeatable*)
    - **ME16** Reference Number Type
  - **ME17** Marital Status
  - **ME18** Lives in Household
    - **ME19** Street Address
    - **ME20** City
    - **ME21** State
    - **ME22** Zip Code
    - **ME23** Telephone Number (*repeatable*)

  - **ME24** English Proficiency
  - **ME25** Preferred Language

- **ME26** Other Parent/Guardian Name
  - **ME27** Relationship to Client
  - **ME28** Date of Birth
  - **ME29** Gender
  - **ME30** Reference Number (*repeatable*)
    - **ME31** Reference Number Type
  - **ME32** Marital Status
  - **ME33** Lives in Household
    - **ME34** Street Address
    - **ME35** City
    - **ME36** State
    - **ME37** Zip Code
    - **ME38** Telephone Number (*repeatable*)
  - **ME39** English Proficiency
  - **ME40** Preferred Language

- **ME41** Other Family Member Name (*repeatable*)
  - **ME42** Relationship to Client
  - **ME43** Date of Birth
  - **ME44** Gender
  - **ME45** Reference Number (*repeatable*)
    - **ME46** Reference Number Type
  - **ME47** Marital Status
  - **ME48** Lives in Household
    - **ME49** Street Address
    - **ME50** City
    - **ME51** State
    - **ME52** Zip Code
    - **ME53** Telephone Number (*repeatable*)
  - **ME54** English Proficiency
  - **ME55** Preferred Language

DATA ELEMENT QUALIFIERS (Q)

Q1	Name Type Qualifier
Q2	Name Component Qualifier
Q3	Birthdate Verification Qualifier
Q4	Street Address Qualifier
Q5	Telephone Number Qualifier

LEVEL 3: OTHER CORE CASE MANAGEMENT DATA ELEMENTS *(To Be Further Developed)*

A: Education (ED)

- **A1** Last Grade Completed/Current Educational Status
- **A2** Special Education Program Indicator
- **A3** (others to be specified)

B: Health (HE)

- **B1** Immunization History
  - **B2** Verification
- **B3** Pregnancy Status
  - **B4** Due Date
  - **B5** Prenatal Care
  - **B6** Pregnancy Program Participation
  - **B7** Smoking
  - **B8** Previous Births
  - **B9** (others to be specified)
- **B10** Medical Alerts
- **B11** (others to be specified)

C: Household Information (HI)

- **C1** Household Size
- **C2** Household Income
  - **C3** Sources of Income (by family member)
    - **C4** Income Assistance Programs Currently Participating
- **C5** Household Needs

D: Risk Indicators (RI)

- **D1** Domicile (Residence) Type
- **D2** History of Criminal Justice Involvement
- **D3** History of Mental Health Intervention
- **D4** (others to be specified)

E: Service Referrals and Encounters (SR)

(Mapped from CISLS evaluation database to INFOLINE taxonomy)

- **E1** Referrals (*repeatable*)
  - **E2** Source
  - **E3** Status
  - **E4** Date of Referral
- **E5** Encounters (*repeatable*)
  - **E6** Provider
  - **E7** Date of Encounter
  - **E8** Encounter Time (in 15 minute intervals)
- **E9** (others to be specified)

F: Pregnancy Outcome (PO)

- **F1** Birth Weight
- **F2** Gestational Age
- **F3** Birth Length
- **F4** Birth Head Circumference
- **F5** (others to be specified)

G: Other Level 3 Data Elements to be Specified

CORE DATA ELEMENTS KEY

AN	Alpha Numeric (format)
ID	Identifier (format)
Format	Describes the type of element (e.g. AN, ID)
Length	Number of characters (minimum,maximum)
Repeat	May occur more than once in the same record

CORE DATA ELEMENT DEFINITION

Element Name:	CLIENT NAME
Element Number:	CL1
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is the client's name in free-form text. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.
Comments:	Element qualifiers are used to identify the type of name (e.g., legal, AKA) and name component (e.g., last, first, middle). If client is known by several names, must include current legal name.
Example:	
Element Qualifiers:	Name Type Qualifier (see Qualifier section) Name Component Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	Yes
Mapping:	
ANSI TS130:	93(IN202)/Name
CSIS Draft:	ST01/Student Name

CORE DATA ELEMENT DEFINITION

Element Name:	DATE OF BIRTH
Element Number:	CL2
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is the client's date of birth in format CCYYMMDD.
Comments:	It has been suggested that CIDC adopt the DHS Data Systems Branch convention of coding as CCYY0701 the birthdates of clients whose actual dates of birth are not known; the CCYY is supplied by the case manager as a best guess.
Example:	19880915 (1988 September 15)
Element Qualifiers:	Birthdate Verification Qualifier (See Qualifier section)
Length:	8,8
Format:	AN
Repeat:	No

Mapping:

ANSI TS130:	1251 (DMG02)/Date Time Period
CSIS Draft:	DE07/Date of Birth

CORE DATA ELEMENT DEFINITION

Element Name: GENDER

Element Number: CL3

Element Level: 1 (Core Linkage)

Last Revised: March 28, 1994

Definition: This is a code indicating the gender of the client.

Comments: Complete ANSI approved code list

F	Female
M	Male
U	Unknown or Not Available (also used in cases of ambiguous gender of newborn infants)

Proposed additions:

X	Unborn

Example:

Element Qualifiers: None

Length: 1,1
Format: ID
Repeat: No

Mapping:

ANSI TS130: 1068 (DMG03)/Gender Code
CSIS Draft: DE19/Gender

CORE DATA ELEMENT DEFINITION

Element Name:	COUNTY OF BIRTH
Element Number:	CL4
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is a code which identifies the county within the state in which the client was born.
Comments:	Source for complete code list: "Counties and Equivalent Entities of the United States or Provinces, Its Possessions, and Associated Areas (FIPS Publication 8-4)" available from the National Technical Information Service. Proposed additions: Codes for Latin American county-equivalents (e.g., condados, jurisdicciones).
Example:	33002 (Albany, N.Y.)
Element Qualifiers:	None
Length:	5,5
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	1096 (IND03)/County Designator
CSIS Draft:	DE10/Place of Birth - County

CORE DATA ELEMENT DEFINITION

Element Name:	STATE OF BIRTH
Element Number:	CL5
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is a code which identifies the U.S./Latin American state or Canadian province in which the client was born.
Comments:	Complete American National Standards Institute (ANSI) code list is in Appendix B of the CSIS Student Data Handbook.
Example:	CA California DE Delaware FL Florida GU Guam BC British Columbia
Element Qualifiers:	None
Length:	2,2
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	156 (IND02)/State or Province Code
CSIS Draft:	DE11/Place of Birth - State or Province

CORE DATA ELEMENT DEFINITION

Element Name:	COUNTRY OF BIRTH
Element Number:	CL6
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is a code identifying the country of birth of the client.
Comments:	Complete American National Standards Institute (ANSI) code list is in Appendix B of the CSIS Student Data Handbook.
Example:	AF Afghanistan CN China US United States or Provinces of America ZZ Unknown or Unspecified Country
Element Qualifiers:	None
Length:	2,2
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	26 (INDO1)/Country Code
CSIS Draft:	DE12/Place of Birth - Country (Country of Origin)

CORE DATA ELEMENT DEFINITION

Element Name:	REFERENCE NUMBER
Element Number:	CL7
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is the identification number by which the client is known by a particular agency or institution. Note that this is a repeating element; case managers should collect as many reference numbers as feasible[1] for each client, thereby improving the likelihood of establishing a definite match between databases.
Comments:	Must be associated with Reference Number Type.
Example:	
Element Qualifiers:	None
Length:	1,30
Format:	AN
Repeat:	Yes
Mapping:	
ANSI TS130:	127 (IN105)/Reference Number
CSIS Draft:	ST03/Student Identification Number

---

[1] The collection and use of client social security numbers remains controversial. The collaboration has agreed that, while the most widely collected reference number and therefore the single best identification number for linkage purposes, the SSN is best subsumed within a more general set of linkage elements. Agencies and institutions which collect social security numbers can use them, but those that do not will be able to provide other ID numbers for linkage purposes.

CORE DATA ELEMENT DEFINITION

Element Name: REFERENCE NUMBER TYPE

Element Number: CL8

Element Level: 1 (Core Linkage)

Last Revised: March 28, 1994

Definition: This code identfies the type of reference or identification number being transmitted.

Comments: Complete ANSI approved codes

48	Agency's Student Number. This is a number assigned by an agency other than the institution sending the record.
49	Family Unit Number. This is an identification assigned to siblings within the same family.
50	State or Province Student Identification Number. A student identification number assigned by the state education agency to students enrolled in state schools.
56	Corrected Social Security Number
57	Prior Incorrect Social Security Number
LR	Local Student Identification Number. A student identification number assigned by a local school or school district.
MV	Migrant Number. This number is assigned by the national Migrant Student Record Transfer System.
SY	Social Security Number

Proposed additions:

10	Birth Certificate Local File Number
11	Birth Certificate State File Number
12	Medi-Cal (Medicare) Identification Number
13	Naturalization Certificate Number
14	Immigration (INS) Document Number

CL8 CONTINUED ON NEXT PAGE

CORE DATA ELEMENT DEFINITION

CL8 CONTINUED FROM PREVIOUS PAGE

15	California State (DHS) Client Index Number
16	Agency's Client Number
17	Health Insurance Claim Number
18	Driver's License/ID Card Number
19	County Welfare ID Number

Example:

Element Qualifiers: None

Length: 2,2
Format: ID
Repeat: No

Mapping:

ANSI TS130: 128 (IN104)/Reference Number Qualifier
CSIS Draft: ST02/Student ID Number TYPE

CORE DATA ELEMENT DEFINITION

Element Name:	MOTHER'S NAME
Element Number:	CL9
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is the name in free-form text of the client's mother. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.
Comments:	
Example:	
Element Qualifiers:	Name Type Qualifier (see Qualifier section) Name Component Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	Yes
Mapping:	
ANSI TS130:	93 (IN202)/Name
CSIS Draft:	PA02/Parent/Guardian Name

CORE DATA ELEMENT DEFINITION

Element Name:	MOTHER'S MAIDEN NAME
Element Number:	CL10
Element Level:	1 (Core Linkage)
Last Revised:	March 28, 1994
Definition:	This is the maiden name in free-form text of the client's mother. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.
Comments:	
Example:	
Element Qualifiers:	Name Type Qualifier (see Qualifier section) Name Component Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	No
Mapping:	
ANSI TS130:	93 (IN202)/Name
CSIS Draft:	PA02/Parent/Guardian Name

CORE DATA ELEMENT DEFINITION

Element Name:	STREET ADDRESS (CLIENT)
Element Number:	ME1
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This data element is used to provide the client's current street address in free-form text. Must be preceded by a street address qualifier.
Comments:	
Example:	
Element Qualifiers:	Street Address Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	No
Mapping:	
ANSI TS130:	166 (N301)/Address Information
CSIS Draft:	DE02/Street Address

CORE DATA ELEMENT DEFINITION

Element Name:	CITY (CLIENT)
Element Number:	ME2
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This free-form text is used to indicate the name of the city in the client's current address.
Comments:	
Example:	
Element Qualifiers:	None
Length:	2,30
Format:	AN
Repeat:	No
Mapping:	
ANSI TS130:	19 (N401)/City Name
CSIS Draft:	DE03/City

CORE DATA ELEMENT DEFINITION

Element Name:	STATE (CLIENT)
Element Number:	ME3
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code designating the North or Latin American state or province portion of the client's current address.
Comments:	Complete American National Standards Institute (ANSI) code list for this element is in Appendix B of the CSIS Student Data Handbook.
Example:	CA California DE Delaware FL Florida GU Guam AB Alberta
Element Qualifiers:	None
Length:	2,2
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	156 (N402)/State or Province Code
CSIS Draft:	DE04/State or Province

CORE DATA ELEMENT DEFINITION

Element Name:	ZIP CODE (CLIENT)
Element Number:	ME4
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code designating the zip code or postal code portion of the client's current address.
Comments:	In the U.S., the source of this code set is the "National ZIP Code and Post Office Directory, Publication 65."
Example:	303024017 92717 02717 47907 K7L 3N6
Element Qualifiers:	None
Length:	3,9
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	116 (N403)/Postal Code
CSIS Draft:	DE05/Zip or Postal Code

CORE DATA ELEMENT DEFINITION

Element Name:	TELEPHONE NUMBER (CLIENT)
Element Number:	ME5
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is the telephone or fax number or other means of contacting the client. Must be associated with a telephone number qualifier.
Comments:	Must be associated with telephone number qualifier.
Example:	2022930161 (202-293-0161) 3174940570 (317-494-0570) 6126924079 (612-692-4079)
Element Qualifiers:	Telephone Number Qualifier (see Qualifier section)
Length:	7,25
Format:	AN
Repeat:	Yes
Mapping:	
ANSI TS130:	364 (PER04)/Communication Number
CSIS Draft:	

CORE DATA ELEMENT DEFINITION

Element Name: ENGLISH PROFICIENCY (CLIENT)

Element Number: ME6

Element Level: 2 (Minimal and Essential)

Last Revised: March 28, 1994

Definition: This is a code used to indicate the English language proficiency of the client.

Comments: Complete code list which has been submitted by CSIS for ANSI approval

1	English Only
2	Fully English Proficient
3	Limited English Proficient
4	Non-English Speaking
5	Status Unknown
6	Redesignated Fluent English Proficient (The student no longer needs language assistance services and is considered proficient enough in English to academically succeed in English-only classes)

Example:

Element Qualifiers: None

Length: 1,1
Format: ID
Repeat: No

Mapping:

ANSI TS130: 1476 (new)/English Proficiency
CSIS Draft: DE16/English Proficiency

CORE DATA ELEMENT DEFINITION

Element Name:	PREFERRED LANGUAGE (CLIENT)
Element Number:	ME7
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code designating the language preferred by the client's parent or guardian for oral and/or written communication.
Comments:	Complete American National Standards Institute (ANSI) code list for this element is in Appendix B of the CSIS Student Data Handbook.
Example:	AR Arabic EN English ES Spanish FR French VI Vietnamese ZH Chinese; Zhongwen
Element Qualifiers:	None
Length:	2,3
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	819 (IND05)/Language Code
CSIS Draft:	DE15/Primary or Native Language

CORE DATA ELEMENT DEFINITION

Element Name: INTERPRETER FLAG

Element Number: ME8

Element Level: 2 (Minimal and Essential)

Last Revised: March 28, 1994

Definition: This is a code used to indicate whether or not an interpreter was used to acquire the information represented in the database record.

Complete code list as proposed

1	Information acquired exclusively through interpreter
2	Information acquired with the occasional assistance of an interpreter
3	Interpreter not used due to unavailability
4	No interpreter required

Comments: Language used by the interpreter should be coded in the Client Preferred Language or Parent/Guardian Preferred Language field.

Example:

Element Qualifiers: None

Length: 0,1
Format: ID
Repeat: No

Mapping:

ANSI TS130: N/A
CSIS Draft: N/A

CORE DATA ELEMENT DEFINITION

Element Name:	RACE/ETHNICITY (CLIENT)
Element Number:	ME9
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code indicating the self-described racial or ethnic background of a client.
Comments:	The ANSI approved code list, which contains a total of five categories (Asian/Pacific Islander, Black, Caucasian, Hispanic, and American Indian/Alaskan Native), is inadequate. CSIS has proposed codes for race/ethnicity which provide a more comprehensive, hierarchical coding structure, as well as interracial categories. Appendix A contains the complete code list as proposed in the *Student Data Handbook*.
Example:	100 ASIAN or PACIFIC ISLANDER 105 Filipino 110 Chinese 120 Japanese 130 Korean 140 Southeast Asian 141 Vietnamese 142 Cambodian 143 Hmong
Element Qualifiers:	None
Length:	1,1
Format:	ID
Repeat:	No
Mapping:	
ANSI TS130:	1109 (DMG05)/Race or Ethnicity Code
CSIS Draft:	DE17/Race or Ethnicity (Country of Origin)

CORE DATA ELEMENT DEFINITION

Element Name:	MARITAL STATUS (CLIENT)
Element Number:	ME10
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code defining the marital status of the client.
Comments:	Complete ANSI approved code list

D	Divorced
I	Single
K	Unknown
M	Married
R	Unreported
S	Separated
U	Unmarried (single/divorced/widowed)
W	Widowed
X	Legally Separated

Example:

Element Qualifiers:	None
Length:	1,1
Format:	ID
Repeat:	No

Mapping:

ANSI TS130:	1067 (DEMG04)/Marital Status Code
CSIS Draft:	DE22/Marital Status

CORE DATA ELEMENT DEFINITION

Element Name:	PRIMARY CONTACT PARENT/GUARDIAN NAME
Element Number:	ME11
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is the name in free-form text of a parent, guardian, or other adult responsible for the client. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.
Comments:	
Example:	
Element Qualifiers:	Name Type Qualifier (see Qualifier section) Name Component Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	No
Mapping:	
ANSI TS130:	93 (PER02)/Name
CSIS Draft:	PA12/Parent/Guardian Contact Name

CORE DATA ELEMENT DEFINITION

Element Name:	RELATIONSHIP TO CLIENT (PRIMARY CONTACT PARENT/GUARDIAN)
Element Number:	ME12
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is a code indicating the primary contact parent/guardian's relationship to the client.

Complete ANSI approved code list

01	Spouse
02	Son or Daughter
03	Father or Mother
04	Grandfather or Grandmother
05	Grandson or Granddaughter
06	Uncle or Aunt
07	Nephew or Niece
08	Cousin
09	Adopted Child
10	Foster Child
11	Son-in-Law or Daughter-in-Law
12	Brother-in-Law
13	Mother-in-Law
14	Brother or Sister
15	Ward
17	Stepson or Stepdaughter
18	Self
19	Child (An adult who is given legal responsibility for a child by a court)
20	Employee
21	Unknown
22	Handicapped Dependent

ME12 CONTINUED ON NEXT PAGE

CORE DATA ELEMENT DEFINITION

ME12 CONTINUED FROM PREVIOUS PAGE

23	Sponsored Dependent
24	Dependent of a Minor Dependent (A child not legally of age who has been granted adult status)
25	Ex-Spouse
26	Guardian
27	Student
28	Friend
29	Significant Other
30	Both Parents (The residence or legal custody of the student is with both parents.)
31	Court Appointed Guardian
32	Mother
33	Father
34	Other Adult
36	Emancipated Minor (A person who has been judged by a court of competent jurisdiction to be allowed to act in his or her own interest; no adult is legally responsible for this minor; this may be declared as a result of marriage.)
37	Agency Representative
ZZ	Mutually Defined

Comments:

Example:

Element Qualifiers: None

Length: 2,2
Format: ID
Repeat: No

Mapping:

ANSI TS130: 1069 (IN106)/Individual Relationship Code
CSIS Draft: PA03/Relationship to Student

CORE DATA ELEMENT DEFINITION

Element Name: DATE OF BIRTH (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME13
same as CL2 - DATE OF BIRTH (CLIENT)

Element Name: GENDER (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME14
same as CL3 - GENDER (CLIENT)

Element Name: REFERENCE NUMBER (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME15
same as CL7 - REFERENCE NUMBER (CLIENT)

Element Name: REFERENCE NUMBER TYPE (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME16
same as CL8 - REFERENCE NUMBER TYPE (CLIENT)

Element Name: MARITAL STATUS (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME17
same as ME10 - MARITAL STATUS (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: LIVES IN HOUSEHOLD (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME18

Element Level: 2 (Minimal and Essential)

Last Revised: March 28, 1994

Definition: This is a code indicating whether the primary contact parent/guardian lives in the same household as the client. In the case of a "yes" response, collecting the address information in the next 4 data elements in unnecessary.

Comments: Complete code as proposed

Y	Yes
N	No
U	Unknown
X	Not Applicable

Example:

Element Qualifiers: None

Length: 1,1
Format: AN
Repeat: No

Mapping:

ANSI TS130: N/A
CSIS Draft: N/A

CORE DATA ELEMENT DEFINITION

Element Name: STREET ADDRESS (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME19
same as ME1 - STREET ADDRESS (CLIENT)

Element Name: CITY (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME20
same as ME2 - CITY (CLIENT)

Element Name: STATE (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME21
same as ME3 - STATE (CLIENT)

Element Name: ZIP CODE (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME22
same as ME4 - ZIP CODE (CLIENT)

Element Name: TELEPHONE NUMBER (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME23
same as ME5 - TELEPHONE NUMBER (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: ENGLISH PROFICIENCY (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME24
same as ME6 - ENGLISH PROFICIENCY (CLIENT)

Element Name: PREFERRED LANGUAGE (PRIMARY CONTACT PARENT/GUARDIAN)

Element Number: ME25
same as ME7 - PREFERRED LANGUAGE (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name:	OTHER PARENT/GUARDIAN NAME
Element Number:	ME26
Element Level:	2 (Minimal and Essential)
Last Revised:	March 28, 1994
Definition:	This is the name in free-form text of a parent, guardian, or other adult (other than the primary contact parent or guardian) responsible for the client. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.
Comments:	
Example:	
Element Qualifiers:	Name Type Qualifier (see Qualifier section) Name Component Qualifier (see Qualifier section)
Length:	1,35
Format:	AN
Repeat:	No

Mapping:

ANSI TS130:	93 (PER02)/Name
CSIS Draft:	PA12/Parent/Guardian Contact Name

CORE DATA ELEMENT DEFINITION

Element Name: RELATIONSHIP TO CLIENT (OTHER PARENT/GUARDIAN)

Element Number: ME27
same as ME12 - RELATIONSHIP TO CLIENT (PRIMARY CONTACT PARENT/GUARDIAN)

Element Name: DATE OF BIRTH (OTHER PARENT/GUARDIAN)

Element Number: ME28
same as CL2 - DATE OF BIRTH (CLIENT)

Element Name: GENDER (OTHER PARENT/GUARDIAN)

Element Number: ME29
same as CL3 - GENDER (CLIENT)

Element Name: REFERENCE NUMBER (OTHER PARENT/GUARDIAN)

Element Number: ME30
same as CL7 - REFERENCE NUMBER (CLIENT)

Element Name: REFERENCE NUMBER TYPE (OTHER PARENT/GUARDIAN)

Element Number: ME31
same as CL8 - REFERENCE NUMBER TYPE (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: MARITAL STATUS (OTHER PARENT/GUARDIAN)

Element Number: ME32
same as ME10 - MARITAL STATUS (CLIENT)

Element Name: LIVES IN HOUSEHOLD (OTHER PARENT/GUARDIAN)

Element Number: ME33
same as ME18 - LIVES IN HOUSEHOLD (PRIMARY CONTACT PARENT/GUARDIAN)

Element Name: STREET ADDRESS (OTHER PARENT/GUARDIAN)

Element Number: ME34
same as ME1 - STREET ADDRESS (CLIENT)

Element Name: CITY (OTHER PARENT/GUARDIAN)

Element Number: ME35
same as ME2 - CITY (CLIENT)

Element Name: STATE (OTHER PARENT/GUARDIAN)

Element Number: ME36
same as ME3 - STATE (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: ZIP CODE (OTHER PARENT/GUARDIAN)

Element Number: ME37
same as ME4 - ZIP CODE (CLIENT)

Element Name: TELEPHONE NUMBER (OTHER PARENT/GUARDIAN)

Element Number: ME38
same as ME5 - TELEPHONE NUMBER (CLIENT)

Element Name: ENGLISH PROFICIENCY (OTHER PARENT/GUARDIAN)

Element Number: ME39
same as ME6 - ENGLISH PROFICIENCY (CLIENT)

Element Name: PREFERRED LANGUAGE (OTHER PARENT/GUARDIAN)

Element Number: ME40
same as ME7 - PREFERRED LANGUAGE (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: OTHER FAMILY MEMBER NAME

Element Number: ME41

Element Level: 2 (Minimal and Essential)

Last Revised: March 28, 1994

Definition: This is the name in free-form text of a family member of the client other than those listed in ME11 and ME26. Names are sent in separate components in the following order: last-name, suffix-name, first-name, middle-name. This element must be preceded by name type and name component qualifiers.

Comments:

Example:

Element Qualifiers: Name Type Qualifier (see Qualifier section)
Name Component Qualifier (see Qualifier section)

Length: 1,35
Format: AN
Repeat: No

Mapping:

ANSI TS130: 93 (PER02)/Name
CSIS Draft: PA02 Parent/Guardian Name

CORE DATA ELEMENT DEFINITION

Element Name: RELATIONSHIP TO CLIENT (FAMILY MEMBER)

Element Number: ME42
same as ME12 - RELATIONSHIP TO CLIENT (PRIMARY CONTACT PARENT/GUARDIAN)

Element Name: DATE OF BIRTH (FAMILY MEMBER)

Element Number: ME43
same as CL2 - DATE OF BIRTH (CLIENT)

Element Name: REFERENCE NUMBER (FAMILY MEMBER)

Element Number: ME45
same as CL7 - REFERENCE NUMBER (CLIENT)

Element Name: REFERENCE NUMBER TYPE (FAMILY MEMBER)

Element Number: ME46
same as CL8 - REFERENCE NUMBER TYPE (CLIENT)

Element Name: MARITAL STATUS (FAMILY MEMBER)

Element Number: ME47
same as ME10 - MARITAL STATUS (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: LIVES IN HOUSEHOLD (FAMILY MEMBER)

Element Number: ME48
same as ME18 - LIVES IN HOUSEHOLD (PRIMARY CONTACT PARENT/GUARDIAN)

Element Name: STREET ADDRESS (FAMILY MEMBER)

Element Number: ME49
same as ME1 - STREET ADDRESS (CLIENT)

Element Name: CITY (FAMILY MEMBER)

Element Number: ME50
same as ME2 - CITY (CLIENT)

Element Name: STATE (FAMILY MEMBER)

Element Number: ME51
same as ME3 - STATE (CLIENT)

Element Name: ZIP CODE (FAMILY MEMBER)

Element Number: ME52
same as ME4 - ZIP CODE (CLIENT)

CORE DATA ELEMENT DEFINITION

Element Name: TELEPHONE NUMBER (FAMILY MEMBER)

Element Number: ME53
same as ME5 - TELEPHONE NUMBER (CLIENT)

Element Name: ENGLISH PROFICIENCY (FAMILY MEMBER)

Element Number: ME54
same as ME6 - ENGLISH PROFICIENCY (CLIENT)

Element Name: PREFERRED LANGUAGE (FAMILY MEMBER)

Element Number: ME55
same as ME7 - PREFERRED LANGUAGE (CLIENT)

CORE DATA ELEMENT DEFINITION

Qualifier Name:	NAME TYPE QUALIFIER
Qualifier Number:	Q1
Last Revised:	March 28, 1994
Definition:	This is a code which identifies the type of name entered.
Comments:	Complete ANSI approved codes

01	Given Name (Name at Birth)
02	Current Legal Name
03	AKA (also known as); Alias or Nickname
04	Name of Record
05	Previous Name (sometimes called Maiden Name of Female Persons)
07	Married Name

Proposed addition:

08	Social Security Name

Length:	2,2
Format:	ID
Repeat:	No

Mapping:

ANSI TS130:	1107 (IN102)/Name Type Qualifier
CSIS Draft:	Q02/Name Type Qualifier

CORE DATA ELEMENT DEFINITION

Qualifier Name: NAME COMPONENT QUALIFIER

Qualifier Number: Q2

Last Revised: March 28, 1994

Definition: This is a code which specifies the part of the person's name entered.

Comments: Complete ANSI approved codes

01	Prefix (e.g., Mr, Mrs, Miss, Dr)
02	First Name
03	First Middle Name
04	Second Middle Name
05	Last Name
06	First Initial
07	First Middle Initial
08	Second Middle Initial
09	Suffix (Jr, Sr, III, Esq, etc.)
12	Combined (Unstructured) Name
14	Name of Agency
15	Maiden or Former Name
16	Composite Name (used if the name cannot be broken into separate parts; formatted with last name sent first)

Length: 2,2
Format: ID
Repeat: No

Mapping:

ANSI TS130: 1104 (IN201)/Name Component Qualifier
CSIS Draft: Q03/Name Component Qualifier

CORE DATA ELEMENT DEFINITION

Qualifier Name:	BIRTHDATE VERIFICATION QUALIFIER
Qualifier Number:	Q3
Last Revised:	March 28, 1994
Definition:	This is a code which indicates the original means or source for verifying a person's date of birth.
Comments:	Codes submitted by CSIS for ANSI approval

08	Birth Certificate (see comments below)
09	Passport
10	Hospital Certificate
11	Affidavit
12	Immigration Document
13	Baptismal or Church Certificate
14	Physician's Certificate
15	Undocumented (no birthdate verification available)

Proposed Additions:

20	Birthdate Estimated
21	Driver's License
22	Military ID

Certified copy of the person's Birth Certificate is the document of choice when confirming date of birth. When confirming with this document, enter Birth Certificate Local File Number as a Reference Number (CL7).

Length:	1,2
Format:	ID
Repeat:	No

Mapping:

ANSI TS130:	1357 (DMG08)/Birthdate Verification
CSIS Draft:	DE08/Birthdate Verification

CORE DATA ELEMENT DEFINITION

Qualifier Name: STREET ADDRESS QUALIFIER

Qualifier Number: Q4

Last Revised: March 28, 1994

Definition: This code indicates which part of the person's current street address is entered in the Street Address fields.

Comments: Complete code list submitted by CSIS for ANSI approval

1	Street number or P.O. box
2	Street name and suffix (e.g. St, Ave, Ct, Ln)
3	Street apartment/room/suite number
4	Street direction or rural route designation (e.g. SW, NE, #7, etc.)

Length: 1,1
Format: ID
Repeat: No

Mapping:

ANSI TS130: New (N301)/Street Address Qualifier
CSIS Draft: Q13/Street Address Qualifier

CORE DATA ELEMENT DEFINITION

Qualifier Name: TELEPHONE NUMBER QUALIFIER

Qualifier Number: Q5

Last Revised: March 28, 1994

Definition: This code identifies the type of communication number which is being sent for the contact person.

Comments: Complete ANSI approved code list

EM	Electronic mail
FT	Federal telecommunications system (FTS)
FX	Facsimile (FAX)
HP	Home phone
TE	Telephone
WP	Work phone

Proposed additions:

PB	Pager/Beeper
MC	Mobile/Cellular phone
NP	Neighbor's phone
NO	None

Length: 2,2
Format: ID
Repeat: No

Mapping:

ANSI TS130: 365 (PER03)/Telephone Number Qualifier
CSIS Draft: Q09/Contact Number

SECTION III: CASE MANAGEMENT INFORMATION SYSTEMS FUNCTIONAL SPECIFICATIONS STANDARDS

This section provides design and functional specifications standards for automated case management information systems (CMIS) for use by local CISLS sites. As envisioned, the CMIS would store, process, and retrieve information about children and family members served, including referrals made and services provided. Sites may achieve these functional specifications standards by:

- upgrading existing systems,
- developing systems internally, or
- purchasing systems from an outside vendor.

These standards are intended to be applicable to any of these approaches.

The standards are presented below in seven functional categories: *system functionality, system design, user interface, system security, management reports, interconnectivity,* and *vendor services, agreements, and training.* As noted in Section I, all standards have been classified as one of three types:

- *primary standards*, those that should be met by all systems, unless a sound professional reason is available to show why it is not necessary, or technically feasible, to do so in a particular case.

- *secondary standards,* desired as goals, but likely to be beyond reasonable expectations in many situations.

- *conditional standards,* the importance of the standard varies with the application, and may be either primary or secondary depending on the situation.

SYSTEM FUNCTIONALITY

These standards describe the general capabilities a CMIS must have to satisfy the basic requirements of a CISLS and effectively meet the needs of case managers.

Standard 3.1: Family-Oriented Record (primary)

A CMIS should employ a family-oriented record approach which has the ability to identify and relate multiple program participants of the same family. A user should be able to:

- access an individual client's record;
- easily locate all other members' records of that client's family who are currently in the system;
- generate summary information of the family constellation; and
- access all information available on each family member, dependent on security clearance.

This mechanism should extend to the reporting and analysis subsystems as well.

Comment

In family focused case management, case managers must have access to information on the entire family. Access to family information allows for identification of family strengths, needs, priorities and high risk behaviors, and is important for individual and program evaluation.

Standard 3.2: Chronological Tracking (primary)

A CMIS should be able to chronologically track all agency involvement with a client including, but not limited to, the following:

- client movement through the various stages of the program (intake, exit, re-entry, etc.);
- service referrals;
- service encounters; and
- client case notes

Comment

It is important that a CMIS track the who, what, and when of the services provided, and that this information be available for presentation in a variety of formats.

The system should track the date of the event, the participants, and all other information relevant to the interaction. Access to this tracking information should be available through querying and reporting functions.

Standard 3.3: Appointment Scheduler/Tickler System (primary)

A CMIS should have an appointment scheduler/tickler system that automatically generates reminders of case manager commitments including, but not limited to, the following:

- routine client appointments (routinely scheduled follow-ups, e.g., 6 month, 12 month, etc.);
- external referral follow-up for clients;
- staff-scheduled meetings or appointments.

This information should be accessible both on-line and through management reports that can be printed for individual case managers or agency-wide over a given specified time period.

Comment

This feature can serve as a case management tool to assist in client and case manager scheduling, and as a management tool for tracking staff workloads. It can also serve as an on-line calendar of events and help staff members (with proper system security access) determine when and where their colleagues are scheduled.

Standard 3.4: Pre-Printed Form Generation (primary)

A CMIS should have the ability to generate and print all required data entry forms. When a client is already in the system, any fields previously entered should appear pre-printed on the forms with room for handwritten changes if necessary.

Comment

This feature not only provides for data entry forms, but produces a hard copy of the form with all current information, thus informing the case manager of the specific data needed and allowing more efficient use of time. Likewise, the case manager avoids the common problem of redundant data collection and the related problem of asking the client's family to provide information previously given.

Standard 3.5: Support For Third Party Reimbursement (primary)

The CMIS should support requirements for agencies serving client populations eligible for Medi-Cal and other third party reimbursement for services in the collection of appropriate data to support these billing requirements.

Comment

With the new regulations that allow LEA's to seek Medi-Cal reimbursement for services falling into the prescribed LEA service categories, it is important that a CMIS support data collection consistent with this and other third party billing efforts.

Standard 3.6: Back-up and Recovery Systems (primary)

Multiple back-up and recovery systems should be in place to guarantee back up of all system files and database files. There should be an automated external back-up utility for both system and database files. In addition, an option should be available to allow the user to back up individual database files.

Comment

A *system back-up* includes all the programs and software packages on the computer's hard disk. *Data back-up* includes only the files containing the CMIS client and agency data files. Murphy's law is particularly applicable to computer systems. Before an agency's data is entrusted to a CMIS, it is imperative that adequate provision is made to recover from a system failure.

Standard 3.7: User System Modification (primary)

User accessible utilities should be included in the CMIS to facilitate changing, adding to, or enhancing the system database such as adding and deleting data elements or fields, renaming or relabelling data elements, incorporating new fields into screens, creating validation tables for new data elements, and creating ad hoc reports.

Comment

Because there will be ongoing changes and additions to data elements, naming conventions, and reporting needs, it is important that these functions can be performed by a system administrator rather than a programmer, to maximize flexibility, efficiency, and cost effectiveness. For security reasons, this function usually would be limited to the system administrator. (See also Standard 3.11)

Standard 3.8: Archiving Data (primary)

A CMIS should have utilities for, and agencies should develop procedures for removing or archiving data on inactive clients from the database to protect clients' right to privacy.

Comment

Data on clients no longer participating in a program may nevertheless continue to serve an ongoing purpose (e.g., fiscal accountability, transition and follow up, or program evaluation). Archiving inactive records, unlike deletion or expunging, serves these needs while simultaneously protecting a client's right to privacy by restricting access to these data.

SYSTEM DESIGN

Often the selection of a CMIS software package is influenced by the hardware or software currently in place at an agency. Other times, hardware is purchased based on the desire to run a particular CMIS package. For the purpose of this report, no specific hardware or software platform is considered to be the standard. Instead, more general system design considerations are given that can be met by several different hardware and software environments including, but not limited to, *DOS, Windows, Apple Macintosh,* and *UNIX* operating systems.

Standard 3.9: Single- and Multi-User Environments (primary)

A CMIS should have the capability of operating in both single-user and multi-user environments.

Comment

Stand-alone systems do not allow simultaneous access to data by more than one user, and often lack the capability for users to simultaneously perform multiple tasks. Multi-user systems allow authorized users to update data and to immediately access information that has been modified by other users. Many organizations that currently have small staffs (one or two case managers) might require only a single stand-alone computer work station to sufficiently serve case management needs. However, to accommodate expansion of programs or staff, it is important that the design allow for easy conversion to a multi-user system at some later point without a loss in continuity of data or methodology.

Standard 3.10: Automated File and Record Locking (primary)

Automated file and record locking facilities must be in place on multi-user systems such that no two users may modify a given record at the same time causing a file update data fault. When two users do attempt to access the same record, one should be allowed access while the other is given a "Record in Use" message.

Comment

Without file and record locking it would be possible for two users to simultaneously edit the same client record. File and record locking prevent this from happening.

Standard 3.11: Open File Structure (primary)

A CMIS should be designed with an open file structure. Specifically, either the system should be designed using a standard fourth generation database file structure, or it should provide appropriate software tools and documentation capable of manipulating the structure of the database.

Comment

Some systems are difficult or impossible to modify. A standard database file structure will ensure that changes to the system are both economically and technically possible, and increase system flexibility to meet unanticipated user needs. (See also Standard 3.7)

Example

Most existing database and spreadsheet programs employ a standard file format such as the *xBase .DBF* format. They come with a set of tools that allow a user to interactively modify the structure of the database, for example, changing a field's length or data type or by adding additional fields without the need for complex programming changes.

Standard 3.12: Modular System Design (secondary)

A CMIS should be designed as a modular system to allow an agency to implement only those modules relevant to its program and to add new modules as additional needs arise.

Comment

An agency should not have to pay for features that it does not need. Likewise, a CMIS must be expandable to meet the growing needs of an agency. An open file structure (Standard 3.11) lends itself to modular system design.

Standard 3.13: Core Linkage Data and Client Search Algorithm (secondary)

The CMIS should contain a client search algorithm employing the core linkage data elements, as described in Section II, to facilitate identification and searching of client records for data sharing.

Comment

Data sharing across agencies requires the necessary linkage elements as well as an appropriate methodology for identifying and locating client records. A client search algorithm should be designed to ensure maximum likelihood of finding a client record from a foreign system and to minimize the potential for false positive finds.

Standard 3.14: Core Data Elements and Standard Definitions (primary)

Regardless of how data are stored and represented in a CMIS, the system should be capable of working with all relevant core data elements, definitions, and codes as described in Section II.

Comment

The ability to speak a common data language facilitates data sharing across agencies.

Standard 3.15: Minimized Redundant Data Entry (primary)

A CMIS should avoid redundant data entry. When a client is already in the system, any fields previously entered should automatically fill the same fields in other input screens.

Comment

A large amount of a case manager's time can be spent filling out paperwork and forms. This feature, along with pre-printed form generation (Standard 3.4), will help minimize the redundant gathering and input of data already in the database.

Standard 3.16: Data Range Checking (primary)

A CMIS should ensure that each datum entered is within an appropriate pre-specified range of values. If a datum is out of range, an authorized user should be permitted to supplement the prescribed value list to allow entry of the new value. For core data elements (as defined in Section II) the new value should conform or roll up to the prescribed core data element taxonomy.

Comment

A CMIS should support data validity, but should not restrict the user to only those data element values considered at the inception of the CMIS. New categories of item responses will undoubtedly be developed.

Example

If a question regarding housing is asked, there might not be a suitable category for the response given. For example, at the time the system was designed, "mobile home" might not have been considered for inclusion as a valid response to this question. In a well-designed CMIS, the user should be able to add this response to the accepted values list without requiring additional programming.

Standard 3.17: Conditional Skipping of Fields (primary)

A CMIS should allow conditional skipping of fields during the data entry process when a response of a certain value indicates that one or more questions should be skipped, or when the user's access privileges preclude entering or modifying this field.

Comment

This feature helps ensure accurate data entry and prevent illogical or contradictory data from being entered.

Example

A data entry screen should skip over fields regarding information about pregnancy outcome if the client was never pregnant.

Standard 3.18: Required Data Fields (primary)

A CMIS should have the ability to require key or mandatory fields to be completed before allowing the user to exit the screen.

Comment

This feature reduces the occurrence of missing data and ensures that key fields are filled that would allow maximum functionality of the data. If data are not available, an explicit "missing" or "not applicable" response is required.

Standard 3.19: Attached Laser Printer (secondary)

A system must have at least one attached laser printer capable of printing the fonts and sizes as required by the reports and form generation utilities of the CMIS.

Comment

New printer technologies have emerged that make use of various fonts and sizes to gain greater efficiency and useability in report and form generation. Appropriate hardware and software should be in place to take advantage of this technology.

Standard 3.20: Multiple Printer Output (secondary)

The system should have the capability of providing direct print output to multiple printers.

Comment

It is possible that a case manager may need to print a file or report at a printer located in a remote office or at another facility.

Standard 3.21: Print Spooling (secondary)

The system should provide print spooling to allow the user to run reports and schedule printing for a later time, or to continue processing concurrently with printing.

Comment

It is important that the system be designed for maximum program staff efficiency. When the system requires the user to wait until printing is completed before continuing ongoing operations, the flow of work is impeded and valuable system resources are disabled.

Standard 3.22: SQL Interface (secondary)

Regardless of the programming language upon which the CMIS is based, an SQL query expression builder and search engine should be included in the package.

Comment

SQL is the industry standard for querying databases (searching databases for a specific set of variables). SQL's primary strength is that it is designed to work across many different database products using precisely the same syntax and format. Having this ability will allow different CMIS systems a method for sharing and exchanging data. An SQL system typically consists of two components:

> The *expression builder*. An interactive user-friendly program that aids a user in constructing a valid request for data that may be in the form of a single data value (e.g. a client's phone number), a list of clients (e.g. records for an entire family), or a summary report.
>
> The *search engine*. When connected to a computer network where different agencies may have different CMIS systems designed with an SQL interface, the search engine is capable of going out over a network and asking other CMIS systems for the data requested.

USER INTERFACE

The user interface is defined as the method employed by the CMIS to interact with the user. User interface specifications cover all aspects of the way the system responds during processes such as data entry, system help, menu selections, and system navigation. The CMIS must be easy to use even for a novice computer user. A graphical user interface (GUI) is preferred, but is not mandatory since many automated systems already in place will not support GUI. The following standards cover the user interface.

Standard 3.23: Consistent Commands (primary)

The CMIS user interface must use consistent commands and navigation operations by using the same icon or user message located in the same place (and color if appropriate) for the same purpose throughout the program.

Comment

Basic interface design requires simple repetitive commands to control identical functions. User skill and acceptance increases when these principles are employed.

Standard 3.24: Status Communication (primary)

The CMIS should support status communication by having an icon, prompt, or message in the same location on all screens to inform the user of the current status of where the user is in the program, and how to move forward, complete an operation, or back out of an operation where these functions are possible.

Standard 3.25: Menus or Decision Trees (primary)

Menus or decision trees should be used to facilitate user interaction with and navigation of the system based on the user's needs.

Comment

Decision trees or menus will be different based on the user's security access code.

Standard 3.26: On-line Help (primary)

The CMIS should have the ability to provide a user with on-line help in the following areas:

- a description of the specific keystrokes or data entry conventions required to navigate the system or perform basic system functions such as a *record save*, *cancel request*, or *exit system*;

- general context-sensitive information for the current user activity (e.g., data entry, query, or report generation);

- specific context-sensitive help for each data entry field on a given screen; and

- search capability on indexed help items for all operations of which the system is capable within a given security access code.

Comment

Context-sensitive help means that the program is aware of what function, screen, and data element the user was working on when the help key was pressed. Once invoked, the help will appear on that specific function. A complete alphabetized index of all help items should be available if a user is not sure on which subject help is needed.

Standard 3.27: Changing Help Messages (conditional)

The help system should be designed in a way such that the system administrator can augment or change the help messages for a given screen or data element.

Comment

Allowing the system administrator to modify the help messages empowers the agency to ensure that the help system is both up to date and reflects specific characteristics unique to the agency.

Standard 3.28: Function Keys (conditional)

Function keys should be mapped to perform specific, commonly-used tasks.

Comment

Function keys minimize keystrokes and increase efficiency and response time.

Standard 3.29: Alternate Data Entry Devices (secondary)

The CMIS should be designed to allow for migration to alternate data entry devices such as optical scanners, portable pen-based notebook computers, or voice-activated entry as the technology becomes available and affordable.

Comment

There are numerous emerging technologies for the capture of data. The CMIS should have a flexible design to be able to eventually utilize more than keyboard or mouse point-and-click entry without major expense.

SYSTEM SECURITY

System security is related to confidentiality. Confidentiality pertains to the way individually identifiable information is maintained, transferred and shared among agencies, organizations, and other individuals. Section IV addresses these issues in more detail. System security is defined as the protection of records from inadvertent or intentional disclosure, unauthorized access, and loss. It is both a procedural and technological issue in automated data systems.

Standard 3.30: Password Protection (primary)

A CMIS should be password protected. The system should be designed such that each system user is assigned their own unique ID and password by the system administrator. Upon logging into the system for the first time a new user should be forced to replace their assigned password with a new one, known only to them. When the system requires that the user enter a password the password should not appear on the screen as it is typed.

Comment

Comprehensive system password protection is the primary mechanism for preventing unauthorized access of agency data. It is essential to provide individual ID and password combinations to prevent the situation where a single common ID/password combination is used and becomes known throughout the agency. Requiring the new user to select their own password reinforces the importance of the confidential nature of their ID/password combination.

Standard 3.31: Multiple Levels of Security (primary)

A CMIS should support multiple levels of security. That is, when a new ID/password combination is assigned by the system administrator, there must exist the capability of restricting what data may be accessed, which reports can be run, and which system functions can be accessed by that individual user. Access levels should include the following:

- No access - all access denied
- Read only - no data editing allowed
- Read/Write - additions or changes to data allowed

- Read/Write/Delete - data record deletion allowed

- Print - user allowed to print data and specified reports

Comment

Supervisors, system administrators, program managers and case managers will all have different data access needs. The system must be able to restrict user access accordingly. For example, the system might be designed so as to limit a case manager's access to relevant caseload reports and data pertaining their own clients, while a supervisor might have password access to all client data and full reports within the system.

Standard 3.32: On-line Security Control (primary)

A system administrator at the local program level should have on-line control of all security features.

Comment

Assignment and deactivation of passwords and assignment of levels of access should be an on-line function restricted to the system administrator.

Standard 3.33: Automatic Screen Blanking/Lockout (primary)

A terminal which remains inactive for more than a user-specified time period should automatically blank the screen and require an authorized password to reactivate.

Comment

Particularly in a public setting, there is the potential for tampering with computer systems by curious minds. Automatically blanking the screen protects unauthorized access in a situation where a case manager is called away from his or her desk for a protracted period of time while running the CMIS.

Standard 3.34: Modem Dial Back (secondary)

A system which allows incoming phone modem access should be set up such that after a valid ID/password combination is entered, the computer will hang-up the phone and dial the user back at a predetermined phone number.

Comment

In the situation where a modem is set up to receive incoming calls, it is not safe to assume that no one will get access to the phone number of a modem and attempt to connect to the system in this manner. By programming the system to call the user back at a specified phone number (e.g. home or satellite office), unauthorized users will not be able to hack into the system from a remote location.

Standard 3.35: Locked System Servers and Terminals (primary)

System servers for multi-user systems should be kept in a locked room. All CMIS terminals should have a lock and key that will prevent unauthorized users from turning the computer on and viewing, deleting, or tampering with system or data files.

Comment

It is insufficient to rely on system passwords in an environment when unauthorized users can access confidential information on a PC-based computer system. Even if a CMIS is password protected, it is still possible to access files, potentially damaging, erasing, or copying them to diskette. A lock and key that prevents the computer from being turned on and prevents unauthorized removal of the computer's cover plate is another safeguard against even the most ardent system hackers.

MANAGEMENT REPORTS

Through summary management reports, a CMIS can give an administrator or case manager a concise overview of an individual case manager's or agency's caseload. This facilitates analyses of the agency's client base and resource planning. A flexible, well-designed reporting system can meet both mandatory and local evaluation reporting requirements, and allow the user the flexibility to obtain and summarize information in ways that may not have been anticipated at the inception of the CMIS.

Standard 3.36: Standard Reports (primary)

The CMIS should provide the following standard reports:

- Client List (alphabetical)
- Client List (by case manager)

- Service Referral Summary (by period, case manager, agency)

- Encounter Summary (by period, case manager, agency)

- Client Demographic Summary (by period, agency)
- Follow-ups Due/Missed (by period, case manager)

- Missing Data Report (by period, case manager)

- Needs Assessment (by client, agency)

- Goals and Outcomes Attainment (by client, period, case manager, agency)

Comment

The list reports above should not be considered a full set of reports for a CMIS. Rather, these represent the minimum set that any case management system should provide.

By period indicates that a user should be allowed to enter a range of dates from which to search the database for records (encounter, referrals, or services) that were generated within that time period.

By case manager, agency indicates that the report should be available by both individual case managers and for the entire agency as a whole.

Standard 3.37: Ad Hoc Reports (primary)

A CMIS should have the capability of allowing an authorized user to fully search the data base and construct ad hoc reports on any relevant variable(s) in the system.

Comment

The process should be a full screen interactive one and not require programming ability. The user should be presented with the variables in the system organized in a menu or hierarchical fashion to construct any Boolean (combination of) conditions inherent to the search. The report should be directable to the screen, printer, or an electronic file for further editing.

While standardized canned reports can go a long way toward helping an agency understand its data, it is important that agencies be able to ask questions of their data that were not anticipated at the time the system was designed. With modern fourth generation report and query software tools, ad hoc report generation has become the standard for data management.

INTERCONNECTIVITY

As existing clients remain in the program, or as they move in and out of the program, there will be a need to annotate case records and to import and export data based upon different systems. The CMIS should be able to use the imported data to assist the case manager in determining program eligibility, and to pass on important information to the relevant administrators and case managers. This section describes the minimum capabilities that a CMIS should have to communicate directly or indirectly with other users and data systems.

Standard 3.38: Data Import and Export (primary)

A CMIS system shall be capable of importing and exporting at least the core linkage and core minimal and essential case management data from and to external systems (Levels I and II data as defined in Section II). No standard data exchange format has yet been determined by the CIDC. In the interim, a tab delimited ASCII format should be employed.

Standard 3.39: Automatic Determination of Program Eligibility (secondary)

A CMIS should implement the algorithms used by local, state, and federal agencies appropriate to the client population being served by the agency to determine eligibility for external program assistance.

Comment

This feature can expedite processing and enable the case manager to better meet their clients' needs by serving as a gateway to a greater range of services.

Standard 3.40: E-Mail, Editor and Report Writer (secondary)

The CMIS should have the internal capability of, or interface with, an E-mail package, word processor, and report writer.

Comment

Each individual in an organization should have access to both local and national electronic mail (E-mail) and electronic bulletin board services. E-mail and bulletin boards can provide a means of connecting remote rural agencies with their peers, and serve as an information conduit to all for the discussion of problems, ideas, and methods. A word processor is necessary both to enter client notes and to generate form and other communication.

It is not essential that the CMIS include each of the utilities listed above, but at least it should be capable of a seamless interface to available proprietary packages that meet CMIS standards.

VENDOR SERVICES, AGREEMENTS, AND TRAINING

Because many agencies will elect to contract with outside vendors for purchase or development of their CMIS, this section, covers aspects of the relationship between an agency and a CMIS vendor. It is critical for an agency to know what it can expect from a vendor in terms of software support and system training.

Standard 3.41: Standard Software Characteristics (conditional)

Any software product should have the following basic characteristics:

- mature product (on the market long enough that it is substantially bug-free);
- supported by a manufacturer, author, or vendor who is financially stable and has been in business for at least several years; and
- well-known, commercially available and have a large enough user base to provide full support and technical assistance/programming.

Comment

While the basic characteristics listed above are important, there are no clear and universally accepted standards by which to apply them. The reader is therefore encouraged to do some research and use discretion in purchasing software.

Standard 3.42: Written Guarantee of Limited Cost-Free Repair (primary)

The vendor of a CMIS should guarantee in writing that any errors in the program will be fixed free of charge for a fixed period of time.

Comment

Software is likely to contain anomalies that often do not show up in the first few months of operation. For this reason it is necessary to ensure that the vendor accepts full responsibility for the correctness and quality of the software provided for a substantial period of time after installation.

Standard 3.43: Other Written Agreements (primary)

The following minimum set of issues should be governed by written agreements between CMIS software and hardware vendors and the agency:

1. Development

    - Agency responsibility for obtaining and transferring information on specifications and design and making decisions on a timely basis should be clarified.

    - Responsibility for product design/redesign needs to be designated.

2. Source code

    - An agreement should be reached which provides that the source code be turned over free of charge should anything occur to prevent the vendor from maintaining or modifying the software in a timely fashion.

3. Training

    - A training agreement should be spelled out in great detail as to whether a "train the trainer" format will be followed or whether the vendor will provide initial and ongoing training as the needs arise. A curriculum and materials should be included.

4. On-going Support

- The vendor support agreement should be spelled out in great detail, including technical support hot lines, user help lines, on-site or modem access, etc.

5. Updates

- Agreement about the cost and frequency of updates should be reached.

6. New Development

- Agreement should be reached about the agency's participation in the development of new modules or enhancements to existing systems and the agency's right to a portion of profit for these changes.

7. Hardware Maintenance

- Agreement should be reached on terms of a hardware maintenance contract between the hardware supplier and the agency.

SECTION IV: CONFIDENTIALITY STANDARDS FOR DATA SHARING AND CASE MANAGEMENT INFORMATION SYSTEMS

INTRODUCTION

In the course of investigating clients' needs and providing client services, agencies often require children and families to share some of the most intimate and private information about themselves. Confidentiality restrictions protect the privacy of individuals and insure that personal information is disclosed only when necessary.

There are a number of reasons for respecting the privacy of children and families:

- Privacy is a fundamental right; clients have a core interest in privacy. They have "the right to be left alone."

- Confidentiality restrictions **protect embarrassing personal information from disclosure.** This information may include histories of emotional instability, marital conflicts, medical problems, physical or sexual abuse, alcoholism, drug use, limited education, or erratic employment.

- Confidentiality provisions also **prevent the improper dissemination of information about children and families that might increase the likelihood of discrimination against them.** By its very nature, such information -- about HIV status, mental health history, use of illegal drugs, or charges of child abuse -- can be harmful if released. In some instances, this harm can occur even if records clearly show that the information is unproven or inaccurate.

- Sometimes protecting confidential information is necessary to **protect family and personal security.** For example, in a domestic violence situation, an abused woman who leaves her home may be in great danger if law enforcement personnel disclose her new location. Many immigrant families may shy away from using public health clinics or other social services for fear that the Immigration and Naturalization Service (INS) will take action against them.

- Restricting information given to human service agencies may also **protect job security.** Some information -- such as a history of mental health treatment -- may have no connection with a person's actual job performance, but may nevertheless jeopardize the individual's position, likelihood of promotion, or ability to find new positions.

- Children and families also want to **avoid prejudice or differential treatment** by people such as teachers, school administrators, and service providers. Teachers may lower their expectations of children they learn are eligible for food stamps or free school lunches. This may set in motion a self-fulfilling prophecy in which lowered expectations lead to lowered performance.

- Confidentiality provisions also may be necessary to **encourage individuals to make use of services designed to help them.** Adolescents may avoid seeking mental health services at a school-based clinic, for example, if they believe that this information will get back to their teachers, parents, or peers. The same holds true for medical consultation for birth control or for diagnosis of HIV.

While it is important to respect the need for privacy and the "right to be left alone," this right must be balanced with the need of agencies to know about their clients in order to serve them effectively and efficiently. Children and families may be involved in several different systems simultaneously. Some families might be better served by more than one agency. In both cases, services are improved from greater cross-system information sharing and collaboration. There are a number of reasons that agencies need access to information from other agencies in order to serve children and families more effectively and efficiently:

- Typically, agencies are charged with providing limited services to children and families. Most children and families at risk, however, have multiple needs. To **conduct comprehensive assessments** of children and family needs, it may be necessary to have access to information from several agencies. This serves the interests of children and families as well as that of the participating agencies.

- To **provide all necessary services** of clients, it is also necessary to share information among agencies. This is also in the interest of children and families as well as agencies.

- Sharing information also helps **coordinate service plans** and **avoid duplication of services**. Despite different missions, various agencies may nevertheless provide similar or overlapping services. The program plans of different agencies may also make conflicting demands on clients. Sharing information avoids wasteful duplication, resolves these conflicts, and frees resources so that agencies are able to provide more comprehensive care for clients.

- As agencies implement family service plans, continued sharing of information will **facilitate monitoring of services** by each agency involved. This monitoring ensures that needed services are actually provided and that agencies are properly reimbursed for mandated services.

- Information-sharing helps to **make services more family-focused**. Individual problems that agencies address often have roots in broader family issues. Information-sharing enlarges the perspective of service needs. It may ultimately be more helpful, for example, to view an individual youth's delinquent behavior in the context of family problems such as unemployment, inadequate housing, substance abuse, and emotional instability. Sharing of information among agencies allows service providers to gain that broader perspective and provide the family with appropriate services.

- Information-sharing also helps agencies reach out to **serve the needs of the broader community.** Statistical analyses may be invaluable in determining the effectiveness of programs in place, current community needs that are unmet, projections of the need for services in the future, and the best ways to allocate limited resources.

How To Use These Standards

These standards attempt to strike a balance between the dual goals of protecting client privacy and sharing client information. They are intended to provide a workable approach to the management of client information maintained by a school-based collaboration project. The standards assume the existence of an automated case management system, although they are intended to apply to all recordkeeping systems and methods of data sharing. While they are consistent with legal protections, the standards do not purport to incorporate every legal or ethical provision concerning the confidentiality of client information or records. Nor do the standards, by themselves, resolve every confidentiality question that may arise in the course of serving families.

In order to analyze a specific confidentiality question, the reader must be familiar with the confidentiality provisions applicable to the information or records at issue. For example, education records are subject to different confidentiality restrictions than those that apply to mental health records. The standards suggest that information maintained by an interagency partnership should be subject to the strictest standards owed by any of the participating agencies. These policies should control the release of confidential information both among the member agencies of the collaboration partnership and to nonparticipating agencies or entities. Each of the standards should be treated as *primary*, as defined in Section I.

Federal and California statutes and regulations relevant to interagency data sharing appear in Appendices B and C. These charts are intended to provide readers and site program staff with more specific information about confidentiality provisions which agencies must adhere to when exchanging client data or developing agreements to do so.

The terms "information," "records" and "data" are used interchangeably throughout this section. The standards are intended to apply to all client information regardless of its form and to all methods of exchanging client information, unless otherwise specified. The term "agency" is used to refer to the service providers participating in the interagency partnership. The terms "partnership" or "collaborative effort" are used to refer to the aggregate collaborative program.

BASIC PRINCIPLES

Standard 4.1: Presumption of Confidentiality (primary)

Agencies should presume that client information and records are confidential and should not disclose the information unless a specific exception to the presumption applies or the disclosure is authorized by the client, a court or another appropriate mechanism.

Comment

Presuming that client information is confidential should always be the starting point for an agency or partnership developing a policy on confidentiality. The presumption helps to frame the analysis of confidentiality provisions. Many layers of confidentiality provisions -- including federal and state statutes, federal and state regulations, and professional privileges -- may apply to the same client data. None of the provisions, however, is absolute. All allow information sharing under certain circumstances. The most common mechanism for exchanging client data is by written consent of the client. Other methods for sharing include court orders addressing confidentiality and sharing permitted expressly by statute. The presumption is a starting point and should not constitute a significant barrier to sharing information for the purposes of collaboration.

Standard 4.2: Satisfy the Strictest Standard Required (primary)

An interagency collaborative effort should satisfy the strictest legal and professional standards for confidentiality owed by any participating agency.

Comment

For many collaborative efforts, the perception that confidentiality provisions inhibit interagency services arises from the confusing demands of different agencies' duties. For example, some agencies protect information that others do not. Some require consent when others allow sharing without consent, or with a less thorough standard release form. By extending the most stringent requirements across agencies participating in the collaboration, the partnership protects client privacy and creates a standard procedure that is easily applied. Applying the most stringent requirements should not prove overly burdensome, nor should it construct impassable barriers. Virtually all client data may be exchanged using authorized mechanisms, such as client consent.

Confidentiality policies and procedures may vary among interagency partnerships along with the services provided, the client information maintained and the agencies participating in the collaborative effort. Moreover, even within a partnership, policies dictating the disclosure of level one data elements may well differ from the policies dictating disclosure of level three data elements because of the increasing sensitivity of the information and the corresponding need to limit its disclosure.

Standard 4.3: Collect Only Necessary Information (primary)

Agencies should collect and record only that information that is genuinely needed to fulfill the goal of serving the client.

Comment

This principle is especially important when agencies employ automated data systems, as seemingly limitless memory capacities may encourage staff to collect and record all interesting information, whether or not it is relevant to the needs of the client. In order to implement this standard, agency personnel must have a clear understanding of the agency's goals and each family's case plan.

In some situations, detailed information should not be included in client files even though it may be relevant. For example, it may be enough to note in a client's record (or in an automated data file) the **fact** that the client received medical care, instead of recording the details of the client's medical condition and course of treatment. If another agency has a valid need for more information about the client's medical history, that agency can obtain a specific release for the medical information from the client.

More information is not necessarily better. Collecting excess and irrelevant information has significant costs and liabilities, including:

- making the sharing of information more difficult and time-consuming;
- increasing the danger of inappropriate and damaging disclosure;

- making the client file bulkier and more cumbersome;
- increasing administrative costs of storage and management; and
- increasing the danger that unreliable or inaccurate information may be shared with other agencies.

Standard 4.4: Informing Clients (primary)

At the initial meeting with each client, or soon after, agency personnel should conduct a thorough and meaningful discussion with the client about the agency's practices with regard to confidential information.

Comment

It is important for clients to realize that the agency respects their privacy and will carefully safeguard their confidential information. If clients trust the agency to be discrete, they will be much more likely to seek services and provide complete information to personnel.

Clients should be notified if certain information about them is being put into an automated data system and that it will be accessible to others for specific purposes. The notice should specify the type of information put into the system, the particular individuals or agencies who will have access to the information, the reasons for which they may have access to the information, and the uses they may make of the information.

Staff who are mandated reporters under the child abuse reporting laws should advise clients at the first interview that they will keep client information confidential *unless* the law requires staff to report the information. This should be part of the initial discussion with the client about matters of confidentiality.

PERMISSIBLE DISCLOSURES

Standard 4.5: Sharing "Non-identifiable" Information (primary)

"Non-identifiable" information may be shared for statistical research or other purposes provided agencies ensure that the information is truly non-identifiable.

Comment

It is important to recognize that several pieces of information that individually would not identify a client may, taken together, identify that client and therefore do not qualify as non-identifying information.

Standard 4.6: Sharing Non-confidential Personal Information (primary)

Agencies should provide clients, in their own language, verbal and written explanations of their practices regarding the sharing of non-confidential personal information.

Comment

Some information, though personal, is not considered confidential. Generally, non-identifiable information is not deemed confidential. The rationale for this is that if the information, though private and perhaps humiliating, needs little protection if it cannot be traced back to the individual. Other information, such as participation in after-school activities, may be considered too trivial for protection in most contexts. It is good practice to inform clients what types of information may be released without their consent.

Standard 4.7: Intra-agency Information Sharing for Administrative Purposes (primary)

Agency personnel may share confidential information within the agency when necessary to fulfill the administrative purposes of the agency.

Comment

For any agency to conduct its business, certain information sharing is necessary among agency personnel in order to properly serve the client and satisfy the agency's legal or contractual obligations. Employees, volunteers, contractors and other individuals working with the agency should be given access to confidential information only when necessary to accomplish their responsibilities within the agency. Anyone given access to confidential information should be subject to agency training requirements and confidentiality precautions.

In large governmental agencies with several departments, the relevant unit for the purposes of information sharing is the department that collected the information.

Thus, information collected by the public benefits department of the social services agency should not be automatically accessible to the child welfare department of the same agency.

Standard 4.8: Mandatory Disclosure in Limited Circumstances (primary)

Agencies should develop policies to promptly discharge their duty to report information required by law.

Comment

State law requires release of otherwise confidential information under specified circumstances. For example, certain professionals are required to report to the state any suspected child abuse. Mental health professionals also have a duty to reveal confidential information if a patient has communicated a serious threat of physical violence against a reasonably identifiable victim or victims -- commonly known as the "Tarasoff" duty. Agencies and partnerships should have clear procedures for identifying information which must be disclosed and for disclosing the information to the proper authorities. Such actions should always be noted in a client's file.

Standard 4.9: Client Consent (primary)

Written consent should be the primary method of obtaining authorization to transfer client information.

Comment

The demands of confidentiality are best met by consulting with the client whose interests are at stake. Virtually all client information can be released with valid client consent. In addition to serving the demands of the law, obtaining client consent helps foster a relationship of trust between the client and the agency and involves the client in the case management process.

Standard 4.10: Obtaining Informed Consent (primary)

Agencies must take steps to ensure that any consent to release confidential information is "informed."

Comment

A written consent form must be in client's primary language. A written release of confidential information in a language not understood by the client, of course, is invalid. The agency should provide an interpreter, if necessary, to supply a thorough explanation of what consent entails. In addition to language difficulty, there may also be cultural barriers to obtaining informed consent. Agency personnel should be aware of cultural customs and attitudes about privacy.

The client's understanding of the need to release information is also critical to the process of obtaining informed consent. Clear notice provides clients with the purposes and extent of the consent they are asked to give. Inadequate and confusing notices may mislead clients and impair the relationship between clients and service providers.

Some statutes have specific requirements for notice to clients regarding release of confidential information.

Clients should understand the kind of information that is likely to be shared, with whom it will be shared and under what circumstances. They should also understand that they are not required to consent, but their refusal to consent may make it difficult or impossible to serve them effectively.

Standard 4.11: Consent of Minors to Release Information (primary)

Agencies should obtain a minor client's consent to release information concerning treatment for which parental consent is not necessary.

Comment

In general, minors (i.e., people under age 18) control information regarding services to which they alone can consent. Since the minor can consent to these services without parental consent, the minor is also considered to control the information regarding the services. Emancipated minors and minors seeking certain types of medical or mental health treatment can consent to their own care.

For all other minors, parental consent is required for medical or mental health treatment. In such cases, agency personnel should assume that the parents control the flow of information about the minor. Under these circumstances, an agency should obtain a parent's consent to share or exchange information.

Standard 4.12: Requirements of Consent (primary)

Consent to release information must always be in writing, should be specific and detailed, and should contain ten components:

1. the name of the person who is the subject of the disclosure;
2. the individual or agency making the disclosure;
3. the individual or agency to receive the information;
4. the purpose of the disclosure;
5. how much and what kind of information are to be disclosed;
6. the signature of the person who is the subject of the information;
7. the date on which the release was signed;
8. a statement advising the client that he or she may revoke the consent at any time except to the extent the agency has already relied on it;
9. a date, event, or condition upon which the consent will automatically expire;
10. a statement that the subject of the information has a right to a copy of the release.

Comment

Although most legal confidentiality provisions do not require that a release contain all of these elements, agencies and partnerships should make it a practice include them. The comprehensive release will satisfy all current requirements for the release of information in the state.

By including all the components, an agency also takes a step toward better interagency collaboration. Through standardization, the client can consent to the release of information and permit all participating agencies to exchange information and coordinate services for the client.

Standard 4.13: Court Orders (primary)

When an agency is unable to obtain client consent, it can share information pursuant to a valid court order.

Comment

Agencies should make every effort to obtain client consent to share information. In unusual circumstances, however, the client might be unavailable or incapacitated, or might refuse to give consent. In these circumstances, if it is essential to share information in order to serve the client, agencies can obtain a court order to release the information. Such orders should always be clear and narrowly-drawn to fit the needs of the participation agencies.

Similarly, agencies may receive court orders or subpoenas requiring them to release otherwise confidential information. Agencies should submit such court orders or subpoenas to an attorney to determine its legality before they release confidential client information.

Standard 4.14: Client Access to Records (primary)

Agencies should inform clients of their right to view and obtain copies of their records.

Comment

Clients should generally have access to the information in their files. Concealing records from clients and hesitation in responding to requests will inevitably breed distrust. There are a few statutory exceptions to the general rule that clients have a right to obtain their own records. For example, some mental health or child welfare records are not automatically accessible by clients.

PROCEDURES TO PROTECT CONFIDENTIALITY

Standard 4.15: Staff Training (primary)

Agencies and partnerships should establish thorough and ongoing programs of staff instruction on issues of confidentiality.

Comment

Frequent and thorough staff training is critical to ensure that agency personnel -- including employees, contractors, volunteers and anyone who has access to client records -- continue to respect the client's right to privacy and adhere to the policies of the agency.

Staff training on confidentiality should include:

- the reasons for ensuring the confidentiality of information about children and families;
- the specific information the agency needs;
- the reasons the agency needs the information;
- information the worker's agency will share with other agencies;
- the purposes of information sharing among agencies;
- the applicable legal provisions, particularly federal and state statutes and regulations;
- the importance of clearly explaining the consent to clients;
- the need for sensitivity to language and cultural issues;
- the requirements of informed consent and the necessary elements for written releases;
- the role of interagency agreements, court orders, and other mechanisms that facilitate interagency information sharing without the consent of clients; and
- special issues that arise from the use of any automated management information system utilized by the agency.

It is especially important that staff members understand both the overall purposes of the interagency collaborative effort, and their agency's role within that partnership. This will assist them in making judgments about the scope of information necessary to fulfill those purposes.

In agencies that use automated data management systems, the importance of staff training cannot be overstated. Since automated systems make so much more confidential information potentially available to so many more workers, the need for regular and comprehensive training is that much greater.

Standard 4.16: Response to Requests for Information (primary)

When individuals or agencies request information about a client, agencies should not provide any client information or even confirm that the client is receiving services unless the agency receives proper authorization to release the information.

Comment

Agencies should be aware that in many cases, especially those where alcohol or drug treatment is involved, the fact that a client is participating in a program may itself be confidential information. In other cases, even if that information is not protected by law, the client may prefer that his or her participation remain confidential. The response to requests for client information might be: "We cannot provide any information whether a particular person received drug treatment services at our agency."

Standard 4.17: Designated Staff Person: "Gatekeeper" (primary)

Agencies or partnerships should appoint one staff member as a "Gatekeeper" to respond to all requests for client information when there is no written release permitting release of the requested information.

Comment

The Gatekeeper should receive specialized training, and develop experience with the issues of confidentiality. He or she should obtain outside advice, such as that of an attorney, when tough questions arise. By centralizing the responsibility for questions concerning confidentiality, agencies make client privacy a high priority and implement sound risk management procedures.

Standard 4.18: Confidentiality Oaths (primary)

Agencies should require all employees to sign a confidentiality oath, pledging not to disclose confidential information discovered in the course of work, as a condition of employment.

Comment

Several statutes require confidentiality oaths, particularly for researchers. Some agencies use staff pledges of confidentiality to promote sensitivity to clients' interests in privacy. The confidentiality oaths are usually written promises to use the information only for designated agency purposes and not to disclose the information to any other person or agency unless specifically authorized.

Standard 4.19: Written Agreements among Agencies (primary)

Interagency partnerships should execute written agreements among the participating agencies to facilitate sharing of client information. Each interagency agreement should specify:

- **what** information will be shared;
- **how** the information will be shared;
- **who** will have access to the information;
- the **purposes** for information sharing;
- **assurances** by participating agencies that they will not disclose the information further except as dictated by the agreement and will resist other efforts to obtain the information; and
- **other requirements** mandated by applicable confidentiality provisions.

Comment

Agencies participating in collaborative partnerships should enter into agreements to spell out the procedure by which they will share client information. These agreements are typically known as memoranda of agreement (MOA), memoranda of understanding (MOU), contracts or interagency agreements. Essentially, they are arrangements between or among agencies to cooperate by exchanging particular information for a specific purpose.Interagency agreements should never provide for an unlimited flow of information among participating agencies. Each agreement should be narrowly drawn to fulfill the purposes of the collaboration.

Some federal and state statutes and regulations authorize agencies to share confidential client information among the members of interagency collaborative efforts without first obtaining client consent. Even though these agencies do not need client consent to share information, it is good practice to inform clients of the nature of the collaborative effort and the manner in which client information will be shared. Moreover, when the collaborative effort is not operating under the auspices of a specific statute that eliminates the need for client consent, the participating agencies are still under an obligation to obtain client consent and the interagency agreement should specifically include the process by which client consent will be obtained.

Standard 4.20: Referrals among Agencies (primary)

When referring a client to another agency for services, the initial agency should inform the client of the referral and alert the receiving agency if confidential client information accompanies the referral.

Comment

Referrals are an integral part of any interagency collaboration, as staff match clients with appropriate agencies. Often confidential client information accompanies the referral. One suggested practice is to follow-up a referral after a short time with a letter to the receiving agency as a reminder of the confidentiality of the information the initial agency collected. This letter has the added benefit of providing a verification that the client actually accepted the referral.

Standard 4.21: Documentation of Disclosure (primary)

Agencies should document all requests for client information and any client information actually released.

Comment

Documenting requests for client information and the response to each request helps to ensure that agency personnel follow established procedures to protect client privacy. Whenever client information is released, a notation should also be made in the client's record or file. Keeping track of the agencies or individuals to whom information is released can assist in monitoring service delivery to clients, responding to client inquiries and managing risk.

The means of documentation could vary according to the method of data exchange. When client data is exchanged in paper form, documentation might consist of a written log as well as a notation in the client's file. If client data is maintained in an agency's data base, the system might include a prompt that requires the sending agency to document and justify release of client data before it is transferred to another data base or downloaded for any purpose.

AUTOMATED SYSTEMS

Standard 4.22: Computerized Information (primary)

In developing a computerized data system and using it effectively, agencies should:

(1) clearly determine the purpose of the computerized system;

(2) obtain the cooperation of all participating agencies;

(3) develop thorough security procedures;

(4) carefully train staff; and

(5) provide notice to children and families.

Comment

The greatest strength of the computer is also its greatest danger: all of the information in all of the files is potentially available in an instant to anyone with a computer terminal. Consequently, automated systems containing client information require more levels and types of security than non-automated systems. This is particularly important because with the rapid growth of technology most agency records will eventually be stored in computers. When an agency's records are linked on a computer network with other agency records for the sharing of information, it must establish safeguards to assure that confidential information is not improperly disclosed.

In determining the purpose of the system, agencies should realize that automated data management systems may have a variety of purposes. Some purposes focus on the **systems** providing services, and include researching needs for services in the community, reporting services provided by particular agencies, evaluating the effectiveness of those services, assessing cost-effectiveness of services, and planning for the future. Other purposes focus on meeting the needs of **individual** clients, and include assisting in comprehensive assessments of client needs, finding services in the community that can meet the client's needs, and tracking the cost of providing those services. Some automated systems may have multiple purposes. It is important to determine the purpose or purposes of the system at the outset, since that choice will affect other aspects of the system, such as accessibility of information, levels of security, and usefulness of the system to administrators, policy makers, and line workers.

Obtaining cooperation of participating agencies often provides a difficult task. Agencies must agree on what kind of hardware and software they will use and how they will insure compatibility. Agencies must also agree on how to identify people in the system (e.g., by a certain numerical code). Although these initial steps seems rudimentary, they have been substantial obstacles for agencies in the past.

Beyond the basic issues of hardware and software compatibility and common identifiers, agencies need to agree on a host of issues such as what information will be entered into the system from each agency, who will have access to the information in the system, how the information may be used by the participating agencies, and which security measures will be instituted to protect confidentiality and the integrity of the system. These issues, once resolved, should be memorialized in an agreement among the participating agencies.

Standard 4.23: Security Procedures for Automated Systems (primary)

Agencies should develop several levels of security to properly safeguard automated data systems.

Comment

Agencies should not overlook the importance of providing security of the physical environment of data. Data tapes and disks should remain in locked rooms when not in use. Access to these materials should be strictly controlled, with chain-of-custody controls on those who move tapes and disks. Agencies should maintain logs for recording the location of all disks and tapes at all times. Access to computers tapped into the data should be limited.

Once the information is in the computer system, agencies should limit access to the data. This is usually done by a series of passwords. Each password allows the user to get deeper into the system according to his or her authorization to have that level of information. Security can be maintained by giving each user only the passwords that allow access to the information that the user has a legitimate need to know. Some information may be sufficiently sensitive that agencies will prefer not to enter it into any computer database that is subject to access from outside agencies.

As noted earlier, Appendices B and C provide charts of federal and California statutes and regulations relevant to interagency data sharing.

APPENDICES

APPENDIX A

CSIS RACE/ETHNICITY CODES

APPENDIX A

Complete Race/Ethnicity code list as presented in the *CSIS Student Data Handbook* (October, 1993 Draft Version).

- **100 ASIAN or PACIFIC ISLANDER**
  - 105 Filipino
  - 110 Chinese
  - 120 Japanese
  - 130 Korean
  - 140 Southeast Asian
    - 141 Vietnamese
    - 142 Cambodian
    - 143 Hmong
    - 144 Laotian
    - 145 Thai
    - 149 Other Southeast Asian
  - 150 Other Asian
    - 151 Asian Indian
  - 160 Polynesian
    - 161 Hawaiian
    - 162 Samoan
    - 163 Tongan
    - 169 Other Polynesian
  - 170 Micronesian
    - 171 Guamanian
    - 179 Other Micronesian
  - 180 Melanesian
  - 190 Other Pacific Islander

- **200 AFRICAN AMERICAN (BLACK)**
  - 210 African American, non-Hispanic origin
  - 250 African American, Hispanic origin
  - 299 Other African American, not native

- **300 CAUCASIAN**
  - 310 Caucasian, non-Hispanic origin
  - 350 Caucasian, Hispanic origin

- **400 HISPANIC/LATINO**
  - 410 Central American
    - 411 Mexican
    - 412 Guatemalan
    - 413 Costa Rican
    - 414 Salvadoran
    - 415 Nicaraguan
    - 416 Panamanian
    - 417 Honduran
    - 429 Other Central American
  - 430 South American
    - 431 Argentinean
    - 432 Bolivian
    - 433 Chilean
    - 434 Colombian
    - 435 Ecuadorian
    - 436 Paraguayan
    - 437 Peruvian
    - 438 Uruguayan
    - 439 Venezuelan
    - 459 Other South American
  - 460 Other Hispanic/Latino
    - 461 Cuban
    - 462 Puerto Rican
    - 463 Dominican
    - 464 Spaniard
    - 499 Other Hispanic/Latino not listed

- **500 AMERICAN INDIAN/ALASKAN NATIVE**
  - 510 North American Indian
  - 570 Central American Indian
  - 580 South American Indian
  - 590 Alaskan Native
    - 591 Eskimo (Caizo)
    - 592 Aleut

- **600 INTER-RACIAL**
  - 610 Asian/Pacific Islander and
    - 611 African American
    - 612 Caucasian

	613	American Indian
	614	Hispanic/Latino
	619	Other Asian/Pacific Islander Combination
620	African American and	
	621	Asian/Pacific Islander
	622	Caucasian
	623	American Indian
	624	Hispanic/Latino
	629	Other African American combination
630	Caucasian and	
	631	Asian/Pacific Islander
	632	African American
	633	American Indian
	634	Hispanic/Latino
	639	Other Caucasian combination
640	Hispanic/Latino and	
	641	African American
	642	Caucasian
	643	American Indian
	644	Asian/Pacific Islander
	649	Other Hispanic/Latino combination
650	American Indian and	
	651	African American
	652	Caucasian
	653	Asian/Pacific Islander
	654	Hispanic/Latino
	659	Other American Indian combination

APPENDIX B

FEDERAL CONFIDENTIALITY STATUTES AND REGULATIONS

APPENDIX B
FEDERAL CONFIDENTIALITY STATUTES AND REGULATIONS

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Aid to Families with Dependent Children (AFDC)	42 USC §602(a)(9); 45 CFR §205.50;	Information concerning applicants or recipients (including names and addresses, social and economic conditions, medical data, and agency evaluation of recipients; and amounts of assistance)	For purposes directly connected with (A) administration of the program or the SSI program (e.g., establishing eligibility, determining amount of assistance, and providing services for applicants and recipients), (B) any investigation, prosecution, civil or criminal proceeding related to administration of the program, (C) administration of any other federal or federally-assisted program providing cash or in-kind services on the basis of need, (D) an audit of the program by a governmental entity, (E) verification to Employment Security Agency or similar agency that an individual has been an AFDC recipient for 90 days or is WIN participant, (F) administration of the state unemployment compensation program	Yes	If subpoena issued for case record or agency representative to testify, court's attention must be called to regulations against disclosure of information.
		Name or address of any applicant or recipient to any federal, state, or local committee or legislative body;	For financial audit of program by governmental entity		
		Lists or names of applicants and recipients	In state plan for assistance under Title I, IVA, X, XIV, or XVI (AABD) of Social Security Act, if state legislation prescribes conditions of public access to records of disbursement of funds and prohibits use of list or names for commercial or political purposes. State or local agency can disclose current address of recipient to law enforcement officer who provides social security number of recipient and demonstrates that recipient is a fugitive felon		
Adoption Assistance and Child Welfare	42 USC § 671(a)(8); 45 CFR §§ 205.50, 1340.14, 1355.21, 1355.30	Same as AFDC	Same as AFDC	Yes	Same as AFDC

BEST COPY AVAILABLE

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Alcohol and Drug Abuse	42 USC §§ 290dd-3, 290ee-3 42 CFR § 2.1 et seq.	Records or other information concerning any patient in a federally-assisted alcohol or drug-abuse program (including identity, diagnosis, prognosis, and treatment)	Internal program communications Communications that don't disclose patient-identifying information Medical emergencies Court-ordered disclosures Patient crimes on program premises or against program personnel Research, audit or evaluation Child abuse and neglect reporting	Yes - must include (l) name of the program, (2) recipient of the information, (3) name of the patient, (4) purpose or need for disclosure, (5) how much and what kind of information will be disclosed, (6) patient may revoke consent, (7) date the consent expires, (8) signature of patient, (9) date consent is signed	Qualified service organization agreement (QSOA) with outside organization providing services to the alcohol or drug treatment program
Computer Matching and Privacy Prevention	5 USC § 552a	Any item, collection, or grouping of personally identifiable information about an individual -- education, financial, medical, criminal, employment -- that is maintained by an agency	To officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties If required under § 552 (Freedom of Information Act) Routine use of the record for the purpose for which it was collected To the Bureau of Census for carrying out a census If the record will be used solely as statistical record, and is transferred in a form that is not individually identifiable To the National Archives and Records Administration To a governmental agency for civil or criminal law enforcement activity To a person showing compelling circumstances of health or safety To either house of Congress or any committee or subcommittee To the Comptroller General Pursuant to court order To a consumer reporting agency	Yes	
		Identifiable information in a computerized matching program used (l) to determine eligibility or compliance with regulations of federal cash or in-kind assistance programs, by applicants, recipients, or service providers, or (2) to recoup payments or delinquent debts under federal benefit programs			Written agreement between the agencies specifying, e.g., purpose and legal authority for conducting the program; justification for program and anticipated results; description of records that will be matched, with starting and ending dates for matching; and procedures for notice to applicants and recipients, verifying information produced, retention and destruction of identifiable records, ensuring security of records, and use of records provided

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Early Intervention Program for Infants and Toddlers (Part H of IDEA)	20 USC § 1480(2); 34 CFR § 303.460	Personally identifiable information (incorporates regulations applying to FERPA)	Same as FERPA	Same as FERPA	Same as FERPA
Family Education Rights and Privacy Act (FERPA)	20 USC § 1232g; 34 CFR Part 99	Educational records which contain information directly related to a student and are maintained by an educational agency or institution "Educational records" does not include personal notes or records of teachers or other school officials, records kept for law enforcement purposes by school security, records relating to school employees, records on post-graduate activities, or certain treatment records of students	To school employees within local school system who have legitimate educational interest in records To school officials in district to which student intends to transfer To federal or state education authorities To persons responsible for determining eligibility, conditions, or compliance with terms for financial aid To anyone required to receive information under state statute in effect prior to November 19, 1974 Educational research organizations, providing confidentiality is assured Accrediting organizations Parents of students who are dependents under Internal Revenue Code Appropriate person in health or safety emergency Directory information (name, address, phone, date/place of birth, field of study, activities, dates of attendance, degrees awarded, etc.)	By parents, or by students over 18 years of age or enrolled in post-secondary program Written consent must specify records to be disclosed, purpose of the disclosure, and party to whom disclosure may be made	Court order or lawfully issued subpoena
Food Stamp Program	7 USC § 2020(e)(8); 7 CFR § 272.1(c)	Information obtained from food stamp applicant or recipient households	To persons directly connected with administration or enforcement of Food Stamp Act, other federal assistance programs, federally-assisted state assistance programs for low-income individuals, or general assistance programs To persons directly connected with programs required to participate in state income and eligibility verification system (IEVS) To persons directly connected with verification of immigrant status of aliens through the Systematic Alien Verification and Entitlements (SAVE) Program To persons directly connected Child Support Program of Social Security Act, and employees of HHS establishing or verifying eligibility for benefits under the Social Security Act To employees of Comptroller General's Office, for audits To law enforcement officials investigating violations of Food Stamp Act Recipients of information must protect against unauthorized disclosure.	Yes	

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Freedom of Information	5 USC § 552(a)(2); 45 CFR Part 5b	Act directs federal executive branch agencies to make records, opinions, manuals and other documents available to the public, except for the following: identifying details that would constitute a clearly unwanted invasion of personal privacy; national security or foreign policy; internal personnel rules and practices exempted by other statute; trade secrets, confidential commercial or financial information; inter- or intra-agency communications that would not be available to the public; personnel and medical files; certain law enforcement records; records related to regulation or supervision of financial institutions; geological and geophysical information and data concerning wells; possible violations of criminal law; law enforcement informant records; FBI records pertaining to foreign intelligence, counterintelligence, or international terrorism	Agency information exempted from disclosure	Release to anyone requires request reasonably describing the records	Lawsuit filed in US District Court
Juvenile Justice and Delinquency Prevention	42 USC § 5676	Program records containing the identity of individual juveniles gathered for purposes pursuant to the statute		Yes	
Maternal and Child Health Services Block Grant	42 CFR § 51a.6	All information as to personal facts and circumstances obtained by the project's staff about recipients of services	Medical audits by the Secretary of HHS Disclosure in summary, statistical or other form that does not identify particular individuals	Yes	

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Medicaid	42 USC § 1396a(a)(7); 42 CFR § 431.300 et seq.	Information concerning applicants or recipients, including names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation of personal information, medical data (including diagnosis and past history of disease or disability), information for verifying eligibility and amount of medical assistance payments, and information for identification of legally liable third party resources	For purposes directly connected with administration of the program, including establishing eligibility, determining the amount of medical assistance, providing services for recipients, and conducting or assisting in civil or criminal proceedings related to the administration of the program Emergency situations (but agency must notify family or individual immediately after supplying information)	Yes	Subpoena [additional req's?]
Runaway and Homeless Youth	42 USC § 5731	Records containing the identity of individual youths shall not be disclosed or transferred to any individual or to any public or private agency			
School Lunch	42 USC § 1758; 7 CFR § 245.8	Publication, posting, or announcement of names of eligible children Overt identification of eligible children by special tokens, tickets or by other means Physical segregation of eligible children by separate dining area, serving line, dining area entrance, or time to consume milk or meals			
Special Education (Part B of IDEA)	20 USC § 1412,1417(c); 34 CFR § 300.560 et seq.	Educational records (same definition as in FERPA)	Same as FERPA	Same as FERPA	Same as FERPA
Women, Infants, and Children (WIC)	42 USC § 1786; 7 CFR § 246.26(d)	Information obtained from program applicants and participants	Persons directly connected with administration or enforcement of the program, including those investigating violations of the WIC program Representatives of public organizations designated by the chief state health officer which administer health or welfare programs that serve people eligible for the WIC program (the organizations may use WIC information only for determining eligibility of WIC applicants and participants for health or welfare programs, and for conducting outreach to WIC applicants and participants) The Comptroller General, for audits		

BEST COPY AVAILABLE

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Youthful Offender	18 USC § 5038	Records of juvenile delinquency proceedings	To another court of law To an agency preparing a presentence report for another court To law enforcement agencies investigating crimes To the director of a treatment agency or facility to which the juvenile has been committed by the court To an agency considering the person for a position immediately and directly affecting national security To any victim of the juvenile delinquency, or if the victim is deceased, to the victim's family (information shall not be released if requested for an application for employment, license, bonding, or any civil right or privilege) If a juvenile is found guilty of certain felonies on two separate occasions, the court shall transmit to the FBI the name, date of adjudication, court, offenses, sentence, and note that the matters were juvenile adjudications		

APPENDIX C

CALIFORNIA CONFIDENTIALITY STATUTES AND REGULATIONS

APPENDIX C
CALIFORNIA CONFIDENTIALITY STATUTES AND REGULATIONS

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Alcohol & Drug Abuse	Business & Professional Code § 156.1	Records and documents of services for alcohol or drug treatment provided to clients.	Director or Chief deputy director may request an examination and audit by department's internal auditor of all services performed.		
Alcohol & Drug Abuse	Health and Safety Code § 11977	Records of any current or former patient in a Department of Alcohol and Drug Program drug abuse treatment program (including identity, diagnosis, prognosis, and treatment).	Between qualified professionals employed by the treatment or prevention program; With qualified medical persons not employed by the treatment program when necessary for true medical emergency; With qualified personnel in order to conduct scientific research, management audits, financial and compliance audits or program evaluation if the person is not identified in any manner.	By client only if purposes of disclosure are stated in a signed consent.	Parent, guardian or conservator of minor, ward or conservatee may designate in writing persons to whom identify in records may be disclosed. If authorized by court of competent jurisdiction after showing probable cause for search warrant.
Child Abuse	Penal Code § 11167	Information relevant to an investigation of child abuse under the Child Abuse and Neglect Reporting Act.	Information may be given to investigator from child protective agency on case, licensing agency investigating case; The identity of the reporter may be disclosed only between child protective services and counsel representing a child protective agency, or to district attorney in a criminal prosecution, or licensing agency when abuse in out-of-home care is reasonably suspected, or when persons waive confidentiality or by court itself;	The reporter may waive his or her anonymity.	Court order
Child Abuse	Penal Code § 11170	Information obtained from the California Department of Justice's index of child abuse reports.	A child protective agency may make information it obtains from the department's index available to reporting medical practitioner, child custodian, guardian ad litem or counsel or appropriate licensing agency if investigating a new case;		

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Child Abuse	Penal Code § 11167.5	Child abuse reports	The following agencies may obtain reports: Multidisciplinary personnel teams; Persons or agencies responsible for licensing of facilities which care for children; The State Department of Social Services or any county licensing agency which had contracted with the state; Hospital scan teams who are trained to identify child abuse; Coroners and medical examiners when conducting a postmortem examination of a child;		Subpoena by the Board of Prison Terms if parole revocation proceedings are pending against a parolee charged with child abuse.
Child Abuse	Welfare & Institutions Code § 350	In a juvenile dependency mediation proceeding, the testimony of a minor may be taken in chambers and outside the presence of the minor's parents but with the parents' counsel present if they have counsel when: (1) testimony in chambers is necessary to ensure truthful testimony; (2) minor is likely to be intimidated in a formal courtroom setting; (3) the minor is afraid to testify before his or her parents. The parents may have the testimony read back or summarized by counsel.			
Child Abuse	Welfare & Institutions Code §§ 830, 10850	Discussions relative to the disclosure or exchange of otherwise confidential information or writings among multidisciplinary child abuse team members.	A member of a multidisciplinary personnel team engaged in prevention, identification and treatment of child abuse may disclose and exchange information and writing regarding incidents of child abuse that may be a part of a juvenile court record in connection with any program of public social services or otherwise designated as confidential under state law if the member of that team reasonably believes it is generally relevant to the prevention, identification, or treatment of child abuse.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Child Abuse	Welfare & Institutions Code § 18961.5	Information regarding families at risk for child abuse or neglect in computerized databases, including only the following: (1) name, address, telephone number and date and place of birth of family members; (2) number assigned to the case by each provider agency; (3) name and telephone number of each employee assigned to the case from each provider agency; (4) date or dates of contact between each provider agency and family member or members.	Information may be only entered into, or disclosed to, provider agency employees designated by the director of each participating provider agency. A provider agency is any agency which has as one of its purposes the prevention, identification, management, or treatment of child abuse or neglect, including social services, children's services, mental health services, probation, law enforcement, and schools.		
Child Custody	Family Code § 3111	Child custody reports prepared by the probation officer, domestic relations investigator or court appointed evaluator.	The report is filed with the court and served on the parties or their attorneys, but is otherwise unavailable.		
Child Custody	Family Code § 3409	Addresses of parties alleging child abuse or domestic violence in custody proceedings which are unknown to the other party.	Addresses are filed only with the court and are otherwise unavailable.		
Child Custody	Family Code § 1818	Family conciliation court information (verbal or written) from parties to the judge, commissioner, or counselor in a proceeding.	Files may be inspected only with written authority of the judge.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Education	Education Code §§ 49061-49078	Pupil records which contain information directly related to a student and are maintained by an educational agency or institution. "Pupil records" does not include informal notes related to a pupil compiled by school officer or employee which are not revealed to any person but a substitute. "Directory information" is not confidential. It includes the name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and most recent public or private school attended.	To school officials and employees within local school systems who have legitimate educational interest in the records; To school officials and employees of other public school systems, including correctional facilities, where student intends or is directed to enroll; To federal or state education authorities where information is necessary to audit an education program provided confidentiality is preserved; To other state and local officials to the extent the information is specifically needed pursuant to a state law adopted prior to November 19, 1974; To parents of students over the age of 18 who are dependents under Internal Revenue Code; To student 16 years or older who has completed 10th grade who requests records; To District Attorney conducting truancy program; To prosecuting agency considering whether parent or guardian has failed to comply with the compulsory education law; To probation officer or district attorney conducting criminal investigation or probation violation investigation; To appropriate persons in an emergency if necessary to protect the health or safety of the student or others; To persons responsible for determining eligibility, or compliance with terms of financial aid; To election officials for voter registration; To accrediting organizations; To research organizations or agencies, if the student is not identified, providing confidentiality is assured; To officials and employees at schools where pupil is enrolled or intends to enroll.	By parent, legal guardian, or the student if over the age of 18.	Court order or lawfully issued subpoena. To police authorities investigating the possible kidnapping of the student subject to the record.

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Education	Education Code § 49602	Any information of a personal nature obtained in school counseling disclosed by a student 12 years or older or by a parent or guardian of student who is receiving counseling from a school counselor.	Discussion with psychotherapists, other health care providers, or school nurse only for referring the pupil for treatment; Reporting of child abuse or neglect; Reporting information to the principal or parents of student when there is a reasonable cause to believe disclosure is necessary to avert a clear and present danger to health, safety or welfare of the pupil or the community; Reporting to principal or other school personnel, parents or others outside the school when it appears a crime with the likelihood of personal injury or significant property losses will or has been committed; To aid in the investigation of a crime;	Yes. If a written waiver is read and signed by the pupil to specified persons, then it may be released. (The information is not part of the student record without the written consent of the person who disclosed the information.) If a written waiver is read and signed by the pupil to specified persons, then it may be released.	Court order.
Education	Welfare & Institutions Code § 401	Information obtained by an educational advocate to assist children in foster care through the educational system.	The advocate must comply with all statutory and regulatory provisions regarding confidentiality. The advocate may obtain transcripts, immunization and school health records, and individual education plans. The advocate may send this information to new schools, as well as to the Department of Social Services to update the child's health and education passport.		
Special Education	Education Code § 56347	All individualized special education programs shall be maintained in accordance with state and federal pupil record confidentiality laws.			

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Civil Code § 56 et seq.	Medical Information that is individually identifiable and in the possession of or derived from a patient's medical history, mental or physical condition or treatment.	A provider of health care may disclose medical information to: (1) Providers of health care or other health care professionals or facilities for purposes of diagnosis or treatment of the patient; (2) An insurer, employer, health care service plan, hospital service plan, employee benefit plan, government authority, or any other person or entity responsible for paying for health care services rendered to the patient, to the extent necessary to allow responsibility for payment to be determined and payment to be made; (3) Any person or entity that provides billing, claims management, medical data processing, or other administrative services for providers; (4) Organized committees and agents of professional societies for medical staffs of licensed hospitals, or to licensed health care service plans, or to professional standards review organizations or to utilization and quality control peer review organizations or to persons or organizations insuring, responsible for, or defending professional liability which a provider may incur; (5) Any private or public body responsible for licensing or accrediting the provider of health care. However, no patient identifying medical information may be removed from the premises except as expressly permitted or required elsewhere by law; (6) The county coroner in the course of an investigation by the coroner's office; or (7) Public agencies, clinical investigators, health care research organizations, and accredited public or private nonprofit educational or health care institutions for bona fide research purposes. No information so disclosed shall be further disclosed by the recipient in any way which would permit identification of the patient.	Authorization must be handwritten or in 8-point or larger type and be clearly separated from other language requiring a signature; Be signed by the patient or a valid representative; State the specific uses and limitations of the information to be disclosed; State the entity disclosing the information; State the entity to receive the information; State the specific uses and limitations of information by the entity to receive the information; State the date after which disclosures cannot be made; State that the signer has a right to receive a copy of the authorization.	A provider of health care shall disclose medical information if the disclosure is compelled by any of the following: (1) A court order; (2) By a board, commission, or administrative agency for purposes of adjudication pursuant to its lawful authority; (3) By a party to a proceeding before a court or administrative agency pursuant to a subpoena, subpoena duces tecum, notice to appear, or any provision authorizing discovery in a proceeding before a court or administrative agency; (4) By a board, commission, or administrative agency pursuant to an investigative subpoena; (5) By an arbitrator or arbitration panel, when arbitration is lawfully requested by either party, pursuant to a subpoena duces tecum or any other provision authorizing discovery in a proceeding before an arbitrator or arbitration panel; (6) By a search warrant lawfully issued to a governmental law enforcement agency.

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Evidence Code § 992, et seq.	Privileged communications between patient and physician, including information obtained by an examination of the patient, transmitted between a patient and his physician in the course of that relationship and in confidence, including diagnoses made and the advice given by the physician in the course of that relationship.	Disclosure for the accomplishment of the purpose for which the physician was consulted; There is no privilege: (1) In the context of certain legal proceedings where the patient has made his or here physical condition an issue; (2) If services were sought or obtained to commit a crime or tort; (3) In certain criminal proceedings; (4) In a proceeding to establish a patient's competence; (5) To provide information for a report required by law.	Yes. Privilege may be waived.	Court order.
Health (Medi-Cal)	Government Code § 12528	Medi-Cal information	The Bureau of Medi-Cal fraud shall make available to federal investigators or prosecutors all information in its possession concerning fraud under the Medi-Cal plan. The Bureau of Medi-Cal fraud shall collect information on a statewide basis regarding cases of abuse and neglect of patient's in health facilities receiving Medi-Cal payments and disseminate its conclusions to local law enforcement agencies and regulatory and licensing authorities.		
Health	Health & Safety Code §§ 199.21 et seq.	Results of HIV tests of identified individuals.	By physician ordering the test to other health care providers (not including health care service plans) for the purposes of diagnosis, care, or treatment. Results of a blood test to detect antibodies of AIDS may be disclosed without written authorization of subject to: (1) The subject of the test or their legal representative; (2) The test subject's provider of health care; (3) An agent or employee of the test subject's provider of health care who provide direct patient care and treatment; and (4) The provider of health care who distributes or uses human body parts donated pursuant to the Uniform Anatomical Gift Act. A physician and surgeon may disclose the results of a confirmed positive HIV test to a person reasonably believed to be a spouse, sexual partner, or person who has shared hypodermic needles after notifying patient of his or her intent to notify the patient's contacts. The county health officer may alert these contacts without disclosing any identifying information about the person believed to be infected or the physician mailing the report.	A separate consent is required for each disclosure. Minors under age 12 may not consent to the release of the results of HIV tests.	By court order if the subject of the test is a dependent of the court.

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Health and Safety Code § 199.34	Results of HIV tests conducted for purposes of research.	The content of any confidential HIV research record shall be disclosed to the research subject, the legal representative of the research subject if the subject is a minor, or the personal representative of a deceased research subject to whom the record pertains 30 days after written request.		
Health	Health & Safety Code § 199.42	Public health records relating to AIDS, containing personally identifying information developed or acquired by state or local public health agencies.	Public health records relating to HIV may be disclosed for public health purposes or by written authorization of the person who is subject of the record. State or local public health agencies may disclose personally identifying information in public health records to other local state or federal public health agencies or corroborating medical researchers when confidential information is necessary to carry out any of the duties of the agency or research in the investigation, control or surveillance of disease.	Yes.	No. No confidential public health records shall be disclosed, discoverable or compelled to be produced in any civil, criminal, administrative or other proceeding.
Health	Health & Safety Code § 199.72	Personal data under the California AIDS Project.			Patient-identifying information may be subpoenaed by the state department but the state department shall seek and the court shall issue a protective order keeping this information confidential.
Health	Welfare and Institutions Code § 1768.9	Results of HIV test required of persons committed to the Youth Authority	The chief medical officer of a facility of the Department of Youth Authority may: (1) Disclose results of an HIV test for the probable causative agent to the superintendent or administrator of the facility where the test is confined. (2) When AIDS test results are positive, inform the test subjects' known sexual partners or needle contacts in a Department of Youth Authority facility of the results as long as the test subject's identity is kept confidential. (3) Place results of the tests in the subjects' confidential medical record, which must be kept separate from other case files and records.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Health & Safety Code §§ 1795 *et seq.*	Personal access to health care records.	An adult patient may examine his or her own records. Any minor patient or the representative of the minor shall be entitled to inspect patient records pertaining only to health care of a type for which the minor is lawfully authorized to consent. Representatives of a minor shall not be entitled to inspect or obtain copies of minor's patient records, however, if (1) the minor has a right of inspection; or (2) health care provider determines that access to the patient's records requested by the representative would have a detrimental effect on the relationship with the minor patient or the minor's physical safety or psychological well-being.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Health & Safety Code § 10125.5	The second section of the certificate of live birth shall be confidential. Such information includes: (1) Birth weight; (2) Pregnancy history; (3) Race and ethnicity of mother and father; (4) Residence address of mother; (5) A blank space for entry of census tract for mother's address; (6) Month prenatal care began and number of prenatal visits; (7) Date of last normal menses; (8) Description of complications of pregnancy and concurrent illnesses, congenital malformation, and any complication of labor and delivery, including surgery; provided that this information is essential medical information and appears in total on the face of the certificate; (9) Mother's and father's occupations and kind of business and industry; (10) Education level of mother and father; (11) Principal source of pay for prenatal care; (12) Expected principal source of pay for delivery; (13) An indication of whether or not the child's parent desires that automatic issuance of a social security number to the child.	Access to portion of certificate of live birth is limited to: (1) The State Department of Health services and staff; (2) The local registrar's staff and local health department staff when approved by the local registrar or local health officer; (3) Persons with valid scientific interest, as determined by state registrar, who are engaged in demographic, epidemiological or other similar studies related to health and who agree to maintain confidentiality; (4) The parent who signed the certificate or, if no parent signed, then the mother; (5) The person named on the certificate; (6) Any person who has petitioned to adopt the person named on the certificate only if he/she can demonstrate that the name and address of the natural parents are necessary to assist him/her in establishing a legal right. Medical necessity will also justify disclosure.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Health	Health & Safety Code § 10805	All other information collected and analyzed under the Birth Defects Monitoring Program besides allowable communication.	Information is available to authorized program staff and persons with a valid scientific interest who meet qualifications determined by the director who are engaged in demographic, epidemiological or other similar health studies and who agree in writing to maintain confidentiality. Information may be provided to others conducting research besides program staff if they are first reviewed and approved by the director and the State Committee for the Protection of Human Subjects. State department of statistical compilations relating to birth defects and miscarriage may be published if they do not identify individual cases or individual sources of information.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Information Practices Act	Civil Code §§ 1798 et seq. (specifically 1798.24 - conditions of disclosure)	No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains. An agency is any state office, officer, department, division, bureau, board or commission, but does not include: the California legislature, an agency established under Article VI of the California Constitution (courts), the State Compensation Insurance Fund or a local agency. An agency may decline to disclose personal information to the person to whom it pertains if the information: (1) Is compiled for the purpose of identifying individual criminal offenders and alleged offenders and consists only of identifying data and notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, release and parole and probation status. (2) Is compiled for the purpose of a criminal investigation of suspected criminal activities. (3) Is contained in any record which could identify an individual and which is compiled at any stage of the criminal law enforcement process. (4) Is maintained for the purpose of an investigation of an individual's fitness for licensure or public employment, or of a grievance or complaint, or a suspected civil offense, so long as the information is withheld only so as not to compromise the investigation.	Agencies may disclose confidential information: (1) To the individual to whom the information pertains; (2) With the prior written voluntary consent of the individual to whom the record pertains, but only if such consent has been obtained not more than 30 days before the disclosure or in the time limit agreed to by the individual in the written consent; (3) To the duly appointed guardian or conservator of the individual or a person representing the individual; (4) To those officers, employees, attorneys, agents, or volunteers of the agency which has custody of the information if the disclosure is relevant and necessary in the ordinary course of the performance of their official duties and is related to the purpose for which the information was acquired; (5) To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties and the use is compatible with a purpose for which the information was collected and the use or transfer is accounted for; (6) To a governmental entity when required by state or federal law; (7) Pursuant to the California Public Records Act; (8) To a person who has provided the agency with advance adequate written assurance that the information will be used solely for statistical research or reporting purposes, but only if the information to be disclosed is in a form that will not identify any individual; (9) Pursuant to a determination by the agency that compelling circumstances exist which affect the health or safety of an individual, if upon the disclosure notification is transmitted to the individual to whom the information pertains at his or her last known address; (10) To the State Archives of the State of California; (11) To any person pursuant to a subpoena, court order, or other compulsory legal process if, before the disclosure, the agency reasonably attempts to notify the individual to whom the record pertains, and if the notification is not prohibited by law; (12) To any person pursuant to a search warrant; (13) Pursuant to Article 3 of Chapter 1 of Division 2 of the Vehicle Code;		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
		(5) Would compromise the objectivity or fairness of a competitive examination for appointment or promotion in public service, or to determine fitness for licensure, or to determine scholastic aptitude. (6) Pertains to the physical or psychological condition of the individual, if the agency determines that disclosure would be detrimental to the individual; (7) Relates to the settlement of claims for work-related illness or injury and is maintained by the State Compensation Insurance Fund; (8) Is required by statute to be withheld from the individual to whom it pertains.	(14) For the sole purpose of verifying and paying government health care service claims; (15) To a law enforcement or regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes; (16) To another person or governmental organization to the extent necessary to obtain information from the person or governmental organization as necessary for an investigation by the agency of a failure to comply with a specific state law which the agency is responsible for enforcing; (17) To an adopted person if the information is limited to general background information pertaining to the adopted person's natural parents, provided that the information does not include or reveal the identify of the natural parents; (18) To a child or a grandchild of an adopted person if disclosure is limited to medically necessary information pertaining to the adopted person's natural parents, provided that the information does not include or reveal the identity of the natural parents; (19) To a committee of the Legislature or to a Member of the Legislature, or his or her staff when authorized in writing by the member, where the member has permission to obtain the information from the individual to whom it pertains or where the member provides reasonable assurance that he or she is acting on behalf of the individual; (20) To the University of California or a nonprofit educational institution conducting scientific research, provided the request for information includes assurances for protecting the confidentiality of the information and assurances that the personal identity of the subject shall not be further disclosed in individually identifiable form; (21) To an insurer if authorized by Chapter 5 of Division 4 of the Vehicle Code; (22) To the protection and advocacy agency designated to protect the rights of persons with developmental disabilities or mental illness, provided the information is limited to: name, address, telephone number and any other information necessary to investigate incidents of client abuse or neglect or to obtain client records.		

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Interagency Programs	Welfare & Institutions Code §§ 18986.40-18986.46	All other information besides that specified under allowable communications.	Persons on children's multidisciplinary services teams within the program may disclose to one another information and records on a child which are relevant to the treatment and services available to that child through the program after a form permitting release of information on child is signed by his or her parent, guardian or legal representative; information exchange is limited to information necessary to formulate client's plan and deliver services. Every member of the children's multidisciplinary team who receives information on children served by the integrated children's services program shall be under the same obligations and subject to the same confidentiality penalties as the person disclosing or providing that information.	Yes. (required).	
			(San Diego) Persons on children's multidisciplinary service team within the program may disclose and view records on a child or child's family if relevant to formulate plan and deliver services. Sharing of information must be governed by a Memorandum of Understanding.	With the written consent of child's parent, guardian or legal representative in San Diego, may release copies of mental health records, physical health and drug and alcohol records.	
Juvenile Justice	Penal Code § 290	Registration of sex offenders which consists of a written statement signed by the offender and his or her fingerprints and photograph.	The statements, photographs and fingerprints required for sex offender registration are not open to inspection by the public or any person other than a regularly employed peace or other law enforcement officer.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Juvenile Justice	Welfare & Institutions Code § 676	**The public shall not be admitted to juvenile court proceedings unless requested by the minor about whom the delinquency petition has been filed and any parent or guardian present.** Upon petition by the probation officer or any other person, the court shall prohibit disclosure of any file or record if it appears that harm to the minor, victims, witnesses, or public from public disclosure outweighs the benefit of public knowledge.	**The judge or referee may admit those persons he or she believes have a direct and legitimate interest in the particular case or work of the court.** Members of public shall be admitted as they would be to trial in a court of criminal jurisdiction, to a hearing concerning petitions filed under Section 602 alleging violation of enumerated violent or serious offenses. Where the petition alleges commission of rape, sodomy, oral copulation or any penetration offense, members of the public will not be admitted to the hearing in either of these circumstances: (1) motion upon request of victim by district attorney for a closed hearing; (2) during victim's testimony if at the time of the offense the victim was under 16. The name of a minor found to have committed one of the enumerated serious offenses shall not be confidential unless the court for good cause orders it to be so. When a petition is sustained for any of the enumerated serious offenses, minutes of proceeding, and orders of adjudication and disposition in the court file shall be available for public inspection, but not any other documents in the file.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Juvenile Justice	Welfare & Institutions Code § 781	Juvenile court records from any proceeding to adjudge a person a ward of the court, to take a minor into temporary custody, or for a minor to appear before a probation officer. Within 5 years after jurisdiction has terminated or after the ward has reached 18 years of age, the ward or probation officer may petition the court to seal juvenile court records. If, after a hearing, the court finds that the ward has not been convicted of a felony or any misdemeanor involving moral turpitude and that rehabilitation has been attained to the court's satisfaction, the court shall order that all court records be sealed. When the ward has been found to have committed one of the serious offenses listed in § 707(b), the court shall not order the records sealed until at least three years have elapsed since the commission of the offense.	In any action or proceeding based upon defamation, a court after showing good cause may order the sealed juvenile records be admitted into evidence. Records are to remain confidential and available for inspection only by the court, jury, parties, counsel for the parties and any other person who is authorized by the court to inspect them. Once the action or proceeding is final, the records shall be sealed again.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Juvenile Justice	Welfare & Institutions Code § 827	A petition filed in any juvenile court proceeding, reports of the probation officer, and all other documents filed in any such case or made available to the probation officer in making his or her report, or to the judge, referee or other hearing officer, and thereafter retained by the probation officer, judge, referee, or other hearing officer. There is a limited exception to juvenile court record confidentiality in cases involving serious acts of violence.	May be inspected only by court personnel, the district attorney, or a city attorney or city prosecutor authorized to prosecute criminal or juvenile cases under state law, the minor who is the subject of the proceeding, his or her parents or guardian, the attorneys for the parties, and any other person who may be designated by court order of the judge of the juvenile court upon filing a petition therefore. Child protective agencies shall also be entitled to inspect these documents upon the filing of a declaration under penalty of perjury stating that access to these documents is necessary and relevant in connection with and in the course of a criminal investigation or a proceeding brought to declare a person a dependent child or ward of the juvenile court. Written notice that a minor enrolled in a public school in kindergarten or grades 1 to 12, inclusive, has been found by a court to have used, sold, or possessed narcotics or a controlled substance or to have committed any crime listed shall be provided by the court, within 7 days, to the superintendent of the school district or attendance, which information shall be expeditiously transmitted to any teacher, counselor, or administrator with direct supervisorial or disciplinary responsibility over the minor whom the superintendent believes needs this information to work with the pupil in an appropriate fashion, to avoid being needlessly vulnerable or to protect other persons from needless vulnerability. If a minor is removed from public school as a result of the court's finding, the superintendent shall maintain the information in a confidential file and shall defer transmittal of the information received from the court until the minor is returned to public school. Each notice sent by the court shall be stamped with the instruction: "Destroy This Record 12 Months After The Minor Returns to Public School. Unlawful Dissemination of This Information Is A Misdemeanor."		

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Juvenile Justice	Welfare and Institutions Code § 828	Information gathered by law enforcement agency regarding juvenile taken into custody. Information regarding escaped minor from secured detention.	Law enforcement agencies may provide information regarding juvenile taken into custody to another law enforcement agency, including school district police or security guard, or to any person or agency which has a legitimate need for the information for purposes of official disposition of a case. When minor escapes from a secure detention facility, law enforcement agency shall release name and any descriptive information about the minor to a person who specifically requests it or without a request if it would be necessary to assist in recapturing the minor or protecting the public from substantial physical harm.		
Juvenile Justice	Welfare and Institutions Code § 1764	Information in the possession of the Youth Authority regarding persons 16 years of age and older who were committed to the Youth Authority by a court of criminal jurisdiction, or who were committed to the Department of Corrections and were transferred to the Youth Authority. Release of information is not authorized if such release could place any person in peril; threaten Youth Authority security; or if the disclosure would violate the California Public Records Act.	Upon request, the following information shall be disclosed to any member of the public, by the director of the Youth Authority or his/her designee: (1) Name and age of person; (2) Court of commitment and offense that was basis of commitment; (3) Date of Commitment; (4) Institution where person is or was confined; (5) Actions taken by paroling authority regarding person, which relate to parole dates; (6) Date person is scheduled to be released to the community; (7) Date person was placed on parole; (8) Date person was discharged from the jurisdiction of the Youth Authority and basis for discharge; (9) When person has escaped from any institution under the jurisdiction of Youth Authority and physical description of person and circumstances of escape.		
Juvenile Justice	Welfare and Institutions Code §§ 1764.1, 1764.2		The director or designee may release the information described in § 1764 regarding a person committed to the Youth Authority by a juvenile court for one of the serious offenses listed in § 676(a) to: (1) Any member of the public who requests the information; or (2) The victim of the offense, the next of kin of the victim, or his or her representative, upon request, if the victim or next of kin is identified in the commitment documents, unless the court has ordered that the information be kept confidential.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Juvenile Justice	Welfare & Institutions Code § 1767.6		In parole revocation proceedings, a parolee or his attorney shall receive a copy of any police, arrest and crime reports pertaining to such proceedings. Portions of such reports containing confidential information need not be disclosed if the parolee or his attorney has been notified that confidential information has not been disclosed.		
Juvenile Justice	Welfare and Institutions Code § 1905	Each youth service bureau shall maintain accurate and complete case records, reports, statistics, and other information necessary for the conduct of its programs. They shall establish appropriate written policies and procedures to protect the confidentiality of individual client records.			
Mental Health	Evidence Code § 1010	Confidential communication between patient and psychotherapist includes information obtained by an examination of the patient, transmitted between the patient and his or her psychotherapist in the course of that relationship and in confidence by a means which, so far as the patient is aware, discloses the information to no third persons other than those present to further the interests of the patient . . . or those to whom disclosure is reasonably necessary for accomplishment of purpose for which psychotherapist was consulted, and includes a diagnosis made and advice given by the psychotherapist in the course of that relationship.	There is no psychotherapist-patient privilege under the following circumstances: (1) When the patient raises the issue of his or her mental status in a legal proceeding. (2) When a psychotherapist is appointed by the court to examine the patient, except upon request by the patient's lawyer in a criminal proceeding. (3) In any proceeding initiated by the defendant in a criminal action to determine his or her sanity. (4) If the psychotherapist has reason to believe that the patient is dangerous to himself or herself or to the property or person of another, and that disclosure of the communication is necessary to prevent the threatened danger. (5) In a proceeding to establish the patient's competence. (6) As to information that the psychotherapist or the patient is required to report to a public employee or that recorded in a public office, if such report or record is open to public inspection. (7) When the patient is under 16 years of age and the psychotherapist has reasonable cause to believe that the patient has been the victim of a crime and disclosure of the communication is in the child's best interest. (8) When the psychotherapist is obligated to make a report of suspected child abuse under the Child Abuse Reporting Act (Penal Code §§ 11164 et seq.).	Yes. Privilege may be waived.	

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Mental Health	Evidence Code § 1014.5	When a minor has requested and been given mental health treatment or counseling to which the minor may consent under Family Code § 6929, the professional person rendering such mental health treatment or counseling has the psychotherapist-patient privilege.			
Mental Health	Health and Safety Code § 1795.14	Mental health records. When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records requested by the patient, the provider may decline to permit inspection or provide copies of the records to the patient, subject to the following conditions: (1) The provider must make a written record of the request and the reasons for denying access. (2) The provider must permit inspection of the records by a physician, surgeon or psychologist designated by the patient. (3) The provider shall inform that patient of the decision to deny access, and inform the patient of his or her right to designate someone to inspect the records. (4) The provider shall indicate in the mental health record whether the patient elected to designate someone to inspect the records.			
Privacy	California Constitution Article I, Section 1	"All persons are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property and pursuing and obtaining safety, happiness and privacy."			

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Privacy	California Vehicle Code § 1808.4	The home address of any of the following persons, that appears in any record of the department, is confidential, if the person requests the confidentiality of that information: (1) Attorney General; (2) State public defender; (3) Members of the Legislature; (4) Judges or court commissioners; (5) District attorneys; (6) Public defenders; (7) Attorneys employed by the Department of Justice, the office of the State Public Defender, or a county office of the district attorney or public defender; (8) Nonsworn police dispatchers; (9) Child abuse investigators or social workers, working in child protective services within a social services department; (10) Active or retired peace officers; (11) Employees of the Department of Corrections, the Department of the Youth Authority, or the Prison Industry Authority; (12) Employees of a city police department or county sheriff's office; (13) Nonsworn employees of federal, state, and local detention facilities (14) Nonsworn personnel in local juvenile halls, camps, ranches, and homes; (15) County counsels assigned to child abuse cases; (16) Investigators employed by the Department of Justice, a county district attorney, or a county public defender; (17) Members of a city council; (18) Members of a board of supervisors; (19) Federal prosecutors and criminal investigators and national park service rangers working in this state; or (20) The spouse or children of persons listed in this section regardless of the spouse or child's place of residence.	The confidential home address of any of the persons listed shall be disclosed to a court, a law enforcement agency, the State Board of Equalization, or any governmental agency to which under any provision of law, information is required to be furnished from records maintained by the DMV. Any of the following DMV records containing confidential home address shall be open to public inspection if the address is completely obliterated or otherwise removed from the record: (1) Records relating to registration of vehicles; (2) Information contained on an application for a driver's license; (3) Abstracts of convictions; (4) Abstracts of accidents.		

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
School Lunch	Education Code § 49557-49559	The governing board of each school district and each county superintendent of schools shall formulate a plan to ensure that the names of children eligible to receive free or reduced priced meals and milk are not published, posted or announced in any manner, or used for any purposes other than the National School Lunch Program. Eligible children shall not be overtly identified by any means. All applications and records concerning any individual, made or kept by any public officer or agency, in connection with the free or reduced price meal eligibility shall be confidential. All statements regarding pregnant or lactating students who qualify for nutrition program supplements are also to be kept strictly confidential.	Records are open for examination for a purpose directly connected with the administration of free or reduced price meal program or any investigation, prosecution or criminal or civil proceeding conducted in connection with the administration of any such program.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services/ Public Benefits	California Department of Social Services: Manual of Policies & Procedures §§ 19-001-19-005.	Name, address and all other information concerning the circumstances of any individual for whom or about whom information is obtained for public social services, including acknowledgement that individual is receiving assistance, is confidential and shall be safeguarded whether written or oral. No disclosure of any information obtained by representative, agent or employee of the county, in the course of his or her duties shall be made to any one other than in the administration of public social services programs. No disclosure of information which identifies by name or address any applicant or recipient or public social services shall be made to federal, state or local legislative bodies and their committees.	Statistical information and social data that is not identified with a particular individual may be released. Confidential information may be released without consent of the applicant/recipient for purposes directly connected with the administration of public social services to: (1) District Attorney or County Counsel; (2) State Department of Social Services, State Department of Health Services and Department of Health, Education and Welfare, and county welfare departments within California; (3) County Auditor; (4) Law Enforcement officials when the applicant/recipient is deceased or when a felony arrest warrant has been issued for the applicant/recipient. Release of such information is limited to data contained within disbursement records for AFDC, special circumstances and social service cases other than child welfare service records; (5) If applicant/recipient sues the state over law governing the administration of public social services, then the attorney representing the state shall have access to all files relating to the plaintiff; (6) To county superintendents of schools and school districts and their representatives, as necessary, for the administration of federally assisted programs which provide assistance in cash, in-hand, or services directly to individuals on the basis of needs; (7) Research organizations if they guarantee in writing that they will meet the conditions and protections of Welfare and Institutions Code § 10850;	Yes. Written consent shall be dated and shall expire one year from the date given unless expressly limited to a shorter period. Telephone authorization may be accepted in lieu of a written consent provided that the applicant/recipient has adequately identified him/herself and should be followed up by a written consent.	

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services/Public Benefits	Unemployment Insurance § 1094-1095	Information obtained in administering unemployment insurance code.	The director shall permit the use of any information in his or her possession to the extent necessary for any of the following purposes: (1) To properly present a claim for benefits; (2) The acquaint a worker or his or her authorized agent with his or her existing or prospective right to benefits; (3) To furnish an employer or his or her authorized agent with information to enable him or her to fully discharge his or her obligations or safeguard his or her rights under this division; (4) To enable an employer to receive a reduction in contribution rate; (5) To enable the Director of Social Services or Director of Health Services, subject to federal law, to verify or determine the eligibility or entitlement of an applicant for, or a recipient of, public social services; (6) To enable county administrators of general relief or assistance to determine entitlement to locally provided general relief or assistance; (7) To enable county district attorneys, or their representatives to seek criminal, civil or administrative remedies in connection with the unlawful application for, or receipt of, public social services; (8) To enable the director or his or her representative to carry out his or her responsibilities under this code; (9) To enable county departments of collection or their representatives to determine entitlement to medical assistance services; (10) To provide any law enforcement agency with the name, address, telephone number, birthdate, social security number, physical description, and names and addresses of present and past employers, of any victim, suspect, missing person, potential witness, or person from whom a felony arrest warrant has been issued, when a request for this information is made by an investigator or peace officer and designated by the head of the law enforcement agency who requests this information in the course of, and as a part of, an investigation into the commission of a crime where there is a reasonable suspicion that the crime is a felony and that the information would lead to relevant evidence;		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
			(11) To provide to, upon written request of, the State Teachers' Retirement System, the Public Employees' Retirement System, or the University Retirement System with information relating to the earnings of any person who is receiving a disability payment from such system; (12) To enable the Federal Department of Health and Human Services, Office of Child Support Enforcement, Federal Parent Locator Service, to administer its child support enforcement programs; (13) To provide county probation departments with wage and claim information in its possession that will assist those departments in the location of victims of crime who, by state mandate or court order, are entitled to restitution that has been, or can be recovered, and to assist in the collection of money owed to the county or the state by any person who has been directed by state mandate or court order to pay restitution, fines, penalties, assessments, or fees as a result of a violation of law; (14) To provide the Student Aid Commission with information concerning any individuals who are delinquent or in default on guaranteed student loans or who owe repayment of funds received through other financial assistance programs administered by the commission; (15) To provide an authorized governmental agency with any or all relevant information that relates to any specific workers' compensation insurance fraud investigation; (16) To enable the Division of Labor Standards Enforcement to seek criminal, civil, or administrative remedies in connection with the failure to pay or unlawful payment of wages; (17) To provide employment tax information to tax officials of Mexico, if a reciprocal agreement exits.		

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services	Unemployment Insurance § 2714	All medical records of the department of social services, except to the extent necessary for proper administration of public social services, are confidential and not to be published or open to public inspection in any way revealing the identity of the claimant or the nature of his or her disability.	The social services department may reveal its records to the Director of Social Services or his or her representatives and may reveal the identity of claimants to the Department of Rehabilitation but the information shall remain confidential and shall not be disclosed except to provide any law enforcement agency with name, address, telephone number, birthdate, social security number, physical description and name and address of present and past employers of any victim, suspect, missing person, potential witness or person for whom felony arrest warrant has been served when request is made by any investigator or peace officer with reasonable suspicion the crime is a felony and information would lead to relevant evidence. The department shall notify all applicants for benefits that release of confidential information from their records will not be protected should there be a felony arrest warrant issued against the applicant or in the event of an investigation by a law enforcement agency.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services/ Mental Health	Welfare & Institutions Code §§ 5328, 5328.01, 5328.7	All information and records obtained in the course of providing either voluntary or involuntary services under the Lanterman Developmental Disabilities Act, Lanterman-Petris-Short Act, Short-Doyle Act or any services subject to Divisions 4, 4.1, 4.5, 5, 6, or 7 of the Welfare and Institutions Code.	Information and records shall be disclosed in the following cases: (1) In communications between qualified professional persons in the provision of services or appropriate referrals, or in the course of conservatorship proceedings; (2) When the patient, with the approval of the physician, licensed psychologist, or social worker who is in charge of the patient, designates persons to whom information or records may be released; (3) To the extent necessary for a recipient to make a claim on behalf of a recipient for aid, insurance or medical assistance; (4) For research, provided that the Director of Mental Health or the Director of Developmental Services designates by regulation, rules for the conduct of research. The rules shall include the requirement that all researchers shall sign an oath of confidentiality. (6) To governmental law enforcement agencies as needed to protect federal and state elective officials and their families; (7) To the Senate Rules Committee or the Assembly Rules Committee for the purposes of legislative investigation authorized by such committee. (8) To the attorney for the patient in any and all proceedings if the patient is unable to sign a release, if the attorney to the satisfaction of the facility identifies himself and that he does represent the interests of the patient; (9) Between persons who are trained and qualified to serve on "multidisciplinary personnel" teams. The information and records sought to be disclosed shall be relevant to the prevention, identification, management, or treatment of an abused child and his or her parents; (10) To the county mental health director or to the director's designee, or to a law enforcement officer or the to the person designated by a law enforcement agency, pursuant to detaining and transporting dangerous or gravely disabled person to facility designated for 72 hour evaluation and treatment; (11) When the patient, in the opinion of his or her psychotherapist, presents a serious danger of violence to a reasonably foreseeable victim or victims, then any of the information or records specified in this section may be released to that person or persons and to law enforcement agencies;	Yes. The consent of the patient, or his or her guardian or conservator shall be obtained before information or records may be disclosed by a professional person employed by a facility to a professional person not employed by the facility who does not have the medical or psychological responsibility for the patient's care. If the recipient of services is a minor, ward or conservatee, his or her parent, guardian, guardian ad litem or conservator may consent to release of information. A separate consent shall be obtained for each separate use with the use specified, the information to be released, the name of the agency or individual to whom the information will be released indicated on the form and the name of the responsible individual who has authorization to release information specified. Other consent provisions: (1) If the recipient of services who applies for life or disability insurance designates in writing the insurer to which records or information may be disclosed; (2) To the attorney for the patient in any and all proceedings upon presentation of a release of information signed by the patient;	Court Order: (1) Information and records may be disclosed to the courts, as necessary to the administration of justice; and (2) Certain state hospital records of certain penal code offenders may be released to law enforcement agencies investigating evidence of a crime upon a showing of probable cause (§ 5328.01)

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
			(12) To persons serving on an interagency case management council, where council has attempted to obtain, but consent is not given, provided that justification why records are necessary is put in client's chart; (13) To a committee established by State Department of Mental Health in the development and administration of a medical quality assurance program governing Short-Doyle Medi-Cal services; (14) The director of a state mental health facility may release information he/she deems essential in aiding the apprehension of certain escapees from a state mental health facility.	(3) Information, except that which was given in confidence by members of the person's family, requested by a probation officer charged with the evaluation of the person after his or her conviction of a crime, provided that such information is relevant to the evaluation; (4) To county patients' rights advocates who have been given knowing voluntary authorization by client or a guardian ad litem; and (5) If the patient gives his or her consent, information specifically pertaining to the existence of genetically handicapping conditions may be released to qualified professional persons for purposes of genetic counseling for blood relatives.	

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services/ Public Benefits	Welfare & Institutions Code §§ 10850, 10850.2, 10850.3, 10850.7	All applications and records relating to any form of social services for which grant in aid are received by this state from the U.S. Government (including names and addresses of applicants to a committee or legislative body or lists of persons receiving public social services).	Any county welfare department in the state may release lists of applicants for, or recipients of, public social services to any other county welfare department of the State Department of Social Services including a housing authority; Any county welfare department and state department of social services shall provide any government entity authorized by law to conduct an audit or similar activity in connection with the administration of public social services with access to any public social services applications and records if used for investigating the administration of public social services and if it does not disclose any names except in cases of criminal or civil proceedings in connection with the administration of public social services; Factual information relating to eligibility provided solely by the public assistance recipient contained in applications and records made or kept by any public officer or agency in connection with the administration of any public assistance program shall be open for inspection by the recipient to which the information relates and by any other person authorized in writing by such recipient. In the event of any hearing involving the applicant or recipient regarding the administration of public social services, the attorney or the authorized representative of an applicant or recipient is entitled to inspect the case record prior to or during the hearing. Information may also be released to: (1) Other public agencies when necessary for verifying eligibility or administration of public social services; (2) County superintendents of schools for administration of federally assisted program; (3) Department of Motor Vehicles; (4) State or local law enforcement agency investigating or gathering information regarding criminal acts committed in welfare department office or against any county or state welfare worker.	Yes. Written authorization shall be dated and signed by the recipient and shall expire one year from the date of execution.	

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
			(5) Law enforcement agencies if a felony warrant has been issued for the arrest of the applicant or recipient, but information released limited to name, address, telephone number, birthdate, social security number and physical description. (6) Law enforcement agencies if applicant or recipient is deceased, but information released limited to name, address, telephone number, birthdate, social security number and physical description. (7) To a child abuse or elder/dependent abuse multidisciplinary personnel team, as defined in Welfare and Institutions Code sections 18951 and 15610.		

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services	Welfare & Institutions Code § 11478.1	All files, applications, papers, documents, and records established or maintained by any public entity pursuant to the administration and implementation of the child and spousal support enforcement program shall be confidential, and shall not be open to examination or released for disclosure for any purpose not directly connected with the administration of the child and spousal support enforcement program. No public entity shall disclose any file, application, paper, document, or record, or the information contained therein, except as expressly authorized by this section.	All files, application, papers, documents and records as described in subdivision (b) shall be available and may be used by a public entity for all administrative, civil, or criminal investigations, actions, proceedings, or prosecutions conducted in connection with the administration of the child and spousal support enforcement program. A document requested by a person who wrote, prepared, or furnished the document may be examined by, or disclosed to, that person or his or her designee. The payment history of an obligor pursuant to a support order may be examined by or released to the court, the obligor, or the person on whose behalf enforcement actions are being taken or that person's designee. Public records concerning the conduct of the people's business such as county standards concerning aid and care for indigent and dependent poor, under the Public Records Act (Gov't. Code § 6250 et seq.). To the extent not prohibited by federal law or regulation, information indicating the existence or imminent threat of a crime against a minor child, or location of a concealed, detained, or abducted child or the location of the concealing, detaining or abducting person, may be disclosed to any district attorney, any appropriate law enforcement agency, or to any state or county child protective agency, or may be used in any judicial proceedings to prosecute that crime or to protect the child. The social security number, most recent address, and the place of employment of the absent parent may be released to an authorized person as defined in Section 653(c) of Title 42 of the United States Code, only if the authorized person has filed a request for the information, and only if the information has been provided to the California Parent Locator Service by the federal Parent Locator Service.		After a noticed motion and a finding by the court, in a case in which enforcement actions are being taken, that release or disclosure to the obligor is required by due process of law, the court may order a public entity, which possesses an application, paper, document, or record as described in subdivision (b) to make that item available to the obligor for examination or copying, or to disclose to the obligor the contents of that item.

BEST COPY AVAILABLE

SUBJECT	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Social Services/Public Benefits	Welfare and Institutions Code § 14100.2, 22 Cal. Code Reg. § 50111	All types of information, whether written or oral, concerning a person, made or kept by any public officer or agency for grants-in-aid received by California from the United States government under Title XIX of the Social Security Act are confidential. Information to be safeguarded regarding applicants and recipients includes: names and addresses, medical services provided, social and economic conditions, agency evaluations of personal information and medical data.	These Medi-Cal records may be viewed for purposes directly connected with the administration of the Medi-Cal program and by the Joint Legislative Audit Committee and the Auditor General for the purpose of investigating or auditing the administration of the Medi-Cal program. The identity of any applicant or recipient shall not be disclosed except in a criminal or civil proceeding conducted in connection with the administration of the Medi-Cal program. The State Department of Health Services may make rules and regulations governing the custody, use and preservation of all records papers, files, and communications pertaining to the administration of medical assistance programs. Regulations set forth in CDSS Policies and Procedures Manual 19 apply to these records (22 CCR § 50111)	Yes.	

CALIFORNIA STATUTES AND REGULATIONS

SUBJECT	CITATION	CONSENT TO MINOR'S MEDICAL TREATMENT	PARENTAL CONSENT OR NOTIFICATION
Alcohol & Drug Abuse	Family Code §§ 6920, 6929	A minor 12 years of age or older may give consent to medical care and counseling relating to the diagnosis and treatment of a drug or alcohol related problem.	Consent of parent or legal guardian is not necessary, except for methadone treatment. The minor's treatment plan shall include the involvement of the minor's parent or guardian, if appropriate. The treatment record shall include statement of whether and when treatment professional contacted minor's parent or guardian, and if not contacted why treatment professional deemed contacting parent or guardian inappropriate.
Health	Health & Safety Code § 1607.5	A minor who is 17 years old may consent to the donation of his or her blood and the penetration of tissue to accomplish such donation.	
Health	Family Code §§ 7002, 7050	A minor emancipated by court order, lawfully married, or on active duty with any of the armed services of the United States of America may give consent to medical, dental or psychiatric care.	Consent of parent or legal guardian is not necessary.
Health	Family Code § 6910	Parent or legal guardian of a minor may authorize in writing any adult person into whose care the minor has been entrusted to consent to medical or dental care.	
Health	Family Code § 6925, Health and Safety Code § 25958	A minor may give consent to medical care related to prevention or treatment of pregnancy. (Does not authorize minor to be sterilized or receive an abortion)	Consent of one of minor's parents, legal guardian, or a juvenile court judge is also necessary to perform an abortion.

SUBJECT	CITATION	CONSENT TO MINOR'S MEDICAL TREATMENT	PARENTAL CONSENT OR NOTIFICATION
Health	Family Code §§ 6920, 6922	A minor 15 years or older who is living separate and apart from his parents or legal guardian, with or without the consent of the parent or guardian and regardless of duration of separation and who is managing his own financial affairs, may give consent to medical or dental care.	Consent of parent or guardian is not necessary. A physician, surgeon or dentist may notify the minor's parent or legal guardian of treatment needed or given.
Health	Family Code §§ 6920, 6926	A minor 12 years of age or older who may have come in contact with any infectious contagious or communicable disease may give consent to hospital, medical and surgical care related to the diagnosis or treatment of such disease if the disease or condition is one required by law or regulation to be reported to the local health officer, or is a related sexually transmitted disease as determined by the State Director of Health Services.	Consent of parent or legal guardian is not necessary.
Health	Family Code §§ 6920, 6927	A minor 12 years of age or older who alleges to have been raped may give consent to medical care related to the diagnosis or treatment of such condition and the collection of medical evidence.	Consent of parent or guardian is not necessary.
Health	Family Code §§ 6920, 6928	A minor who is alleged to have been sexually assaulted may give consent to medical care related to the diagnosis and treatment of such condition and the collection of medical evidence.	Consent of parent or legal guardian is not necessary. However, professional person providing medical treatment shall attempt to contact minor's parent or guardian unless the professional reasonably believe that the minor's parent or guardian committed the sexual assault on the minor.

SUBJECT	CITATION	CONSENT TO MINOR'S MEDICAL TREATMENT	PARENTAL CONSENT OR NOTIFICATION
Mental Health	Family Code §§ 6920, 6924	A minor 12 years or older, who in the opinion of attending professional person, is mature enough to participate in mental health treatment or counselling if he/she: (1) would present a danger of serious physical or mental harm to themselves or others without treatment; or (2) is the alleged victim of incest or child abuse may give consent to outpatient or residential shelter services.	Consent of parent or legal guardian is not necessary. Professionals offering residential services must make best efforts to notify parents. The minor's treatment plan shall include the involvement of the minor's parent or guardian, if appropriate. The treatment record shall include statement of whether and when treatment professional contacted minor's parent or guardian, and if not contacted why treatment professional deemed contacting parent or guardian inappropriate.

REFERENCES

REFERENCES

California Student Information Services and the California Department of Education. (October 1993). *Student Data Handbook.*

Committee on the Standardization of Postsecondary Education Electronic Data Exchange, American Association of Collegiate Registrars and Admissions Officers, Exchange of Permanent Records Electronically for Students and Schools, National Center for Education Statistics, and the Council of Chief State School Officers. (March 1992). *A Guide to the Implementation of the SPEEDE/ExPRESS Electronic Transcript,* Version 1.

Information and Referral Federation of Los Angeles County, Inc. (INFO LINE) and the Alliance of Information and Referral Systems. (1991). *A Taxonomy of Human Services: A Conceptual Framework with Standardized Terminology and Definitions for the Field,* Second Edition.

Soler, M.I.; Shotton, A.C.; & Bell, J. R. (1993). *Glass Walls: Confidentiality Provisions and Interagency Collaborations.* San Francisco, CA: Youth Law Center.